S. HRG. 110–1179

PRIVACY IMPLICATIONS OF ONLINE ADVERTISING

HEARING

BEFORE THE

COMMITTEE ON COMMERCE, SCIENCE, AND TRANSPORTATION UNITED STATES SENATE

ONE HUNDRED TENTH CONGRESS

SECOND SESSION

JULY 9, 2008

Printed for the use of the Committee on Commerce, Science, and Transportation

U.S. GOVERNMENT PRINTING OFFICE

76–329 PDF WASHINGTON : 2012

For sale by the Superintendent of Documents, U.S. Government Printing Office
Internet: bookstore.gpo.gov Phone: toll free (866) 512–1800; DC area (202) 512–1800
Fax: (202) 512–2104 Mail: Stop IDCC, Washington, DC 20402–0001

SENATE COMMITTEE ON COMMERCE, SCIENCE, AND TRANSPORTATION

ONE HUNDRED TENTH CONGRESS

SECOND SESSION

DANIEL K. INOUYE, Hawaii, *Chairman*

JOHN D. ROCKEFELLER IV, West Virginia	TED STEVENS, Alaska, *Vice Chairman*
JOHN F. KERRY, Massachusetts	JOHN MCCAIN, Arizona
BYRON L. DORGAN, North Dakota	KAY BAILEY HUTCHISON, Texas
BARBARA BOXER, California	OLYMPIA J. SNOWE, Maine
BILL NELSON, Florida	GORDON H. SMITH, Oregon
MARIA CANTWELL, Washington	JOHN ENSIGN, Nevada
FRANK R. LAUTENBERG, New Jersey	JOHN E. SUNUNU, New Hampshire
MARK PRYOR, Arkansas	JIM DEMINT, South Carolina
THOMAS R. CARPER, Delaware	DAVID VITTER, Louisiana
CLAIRE MCCASKILL, Missouri	JOHN THUNE, South Dakota
AMY KLOBUCHAR, Minnesota	ROGER F. WICKER, Mississippi

MARGARET L. CUMMISKY, *Democratic Staff Director and Chief Counsel*
LILA HARPER HELMS, *Democratic Deputy Staff Director and Policy Director*
CHRISTINE D. KURTH, *Republican Staff Director and General Counsel*
PAUL NAGLE, *Republican Chief Counsel*

CONTENTS

PRIVACY IMPLICATIONS OF ONLINE ADVERTISING

WEDNESDAY, JULY 9, 2008

U.S. SENATE,
COMMITTEE ON COMMERCE, SCIENCE, AND TRANSPORTATION,
Washington, DC.

The Committee met, pursuant to notice, at 10 a.m., in room SR–253, Russell Senate Office Building, Hon. Byron L. Dorgan, presiding.

OPENING STATEMENT OF HON. BYRON L. DORGAN, U.S. SENATOR FROM NORTH DAKOTA

Senator DORGAN. We are going to begin the hearing this morning. This is a hearing of the Senate Commerce Committee. I am going to begin the hearing now. We will have other Senators join us, but at the moment there is scheduled a series of five votes beginning at 11:15. That may slip a bit. It may slip to 11:30, which means that I would have until 11:45 to leave the room in order to still make the vote. That would give us an hour and 45 minutes. If we do not finish the hearing in an hour and 45 minutes, we will have to recess. The recess will last at least an hour to an hour and a half because five votes take that long.

So my hope would be that we can finish this hearing in about an hour and 45 minutes. I do not want to shortchange the subject. This is a very important subject. We will be holding another hearing on this subject, but for now, as an opening, I want to at least give an opening statement, and then I am going to call on all of the witnesses to provide the testimony. And then we will have time for questions by Senators who come to the hearing.

I want to thank all of you for joining us today to discuss an important topic of privacy in the context of marketing for online advertising. The Commerce Committee has always had an interest in this subject of protecting privacy and doing so in a way that is thoughtful and appropriate. And we need to take a closer look, I think, at Internet users' privacy as the field of online advertising develops.

I understand, first of all, there are many, many benefits to online advertising. I understand that the free Internet and the open architecture of the Internet allows Internet service providers and Internet companies to provide services and products and information in a way that is almost breathtaking, and I understand the backbone of much of that is supported by advertising, by online Internet advertising.

The questions that we discuss and raise today are not meant to suggest that advertising has no value as it relates to the Internet. Quite the contrary is the case. But I think there are issues that are developing that are important issues and those are issues about the invisibility of data collection, the collection of information about online users, the security of the information that has been collected, and the use of that information. I am concerned about the ability of users of the Internet to choose to allow others access to their data with an understanding of where it will be transferred and how it will be used. I am concerned about the users' ability to control this information.

Most of the discussion about advertising on the Internet these days is about—not all of the discussion, but most of it is about behavioral advertising. The companies that have been gathering information about those who use the Internet are companies that wish to find ways to better target advertising.

I was actually this morning visiting with my college-aged daughter about this subject, and she was asking about the hearing. And I said, well, think about going to a big shopping center and going to four stores, and you stop at the cosmetics section, you stop at the shoe section, you shop for a dress, and you go to CVS, and there is someone behind you with a notebook making notes about every place you are stopping and the products you are searching and looking at. That becomes part of a data bank they send to someone.

Well, that is what happens in many cases now with respect to your use of the Internet. Someone is gathering information about where you traveled and what you viewed, and that goes into a data bank and it can be sold or resold and becomes the process by which companies will use the information in which to target advertising directly to you.

I think that the issue here of privacy, who is collecting what kind of information, how does that information exist in what identifiable form or how might that be used, who is it sold to, does the consumer know, all of those issues I think are very, very important. And the issues that surround them I think need to be discussed by the Congress in the context of trying to decide are there protections, further protections, necessary, not only what protections now exist, but are further protections necessary.

Companies believe that by gathering information about online users, they can serve more relevant advertisements to individuals and increase the amount that they can charge per ad. And I understand all that. And revenue is important to the operation of diverse websites, but it is also important for us to ask the questions about protection for users' privacy and whether they should have a choice about whether they want to have data shared about what they are doing on the Internet.

There is some discussion about self-regulation, and the principles proposed by the Federal Trade Commission I think some would suggest are a good start. Some would suggest they are short of what is necessary. The FTC might need to go further and ensure the enforcement of any guidelines. Congress may need to address our patchwork of privacy laws because all of this is a developing

area, and when you are talking about the individual's right to privacy, it is very, very important.

I do want to mention additionally that I had invited the Internet service providers to testify today, and they declined the invitation. So I am going to do another hearing and that hearing will only be with the Internet service providers because I think they have to be a part of this discussion.

I do appreciate all of those who have decided to come at our invitation and give us their perspective on these important issues. And we are going to begin today by hearing from Lydia Parnes, who is the Director of the Bureau of Consumer Protection at the Federal Trade Commission. Then I have asked the panelists to be seated at the table, and we are going to hear from all of those on panel two and then we will ask questions.

I say to Senator Vitter I do not want to do opening statements. I will be happy to recognize you for a moment, but what I want to do—we have a vote starting at 11:15. What I would like to do—if that slips, we may be able to stay here until 11:45, but I want to get all the witnesses to testify and then have an opportunity for questions.

Senator VITTER. All right.

Senator DORGAN. All right.

Ms. Parnes, you have testified before this Committee before. We appreciate your being here again. Let me ask consent, as I recognize you, for the statement by Senator Inouye to be made a part of the permanent record.

[The prepared statement of Senator Inouye follows:]

PREPARED STATEMENT OF HON. DANIEL K. INOUYE, U.S. SENATOR FROM HAWAII

In the United States of America, privacy is a treasured right, but it is also a right that seems to come under regular attack.

Today, commercial entities using digital means can track nearly all of our marketplace moves. Websites and Internet service providers can watch where we go online, what we purchase over the web, and where we linger on the Internet.

Too many consumers spend time on the Internet without knowledge or notice that they are under commercial surveillance. They assume they are in the privacy of their own home and that this privacy will be respected. Unfortunately, this is not always the case.

I am troubled by the current state of affairs. I fear that our existing patchwork of sector-specific privacy laws provides American consumers with virtually no protection. At the same time consumers in other countries are treated with more respect and concern by the very same companies who so freely collect our most private information without warning.

American consumers deserve better. With so much of our commerce and entertainment migrating to the Internet, consumers should not be asked to surrender their privacy each time they go online.

Ensuring that every consumer's right to privacy is appropriately protected will require the Congress's continued attention. Today's hearing on privacy and online advertising represents merely a start, and I look forward to holding additional hearings on these matters later this year.

Senator DORGAN. Ms. Parnes, you may proceed. We have asked all of you to take 5 minutes for your oral testimony, and the permanent record will include your full statements.

STATEMENT OF LYDIA B. PARNES, DIRECTOR, BUREAU OF CONSUMER PROTECTION, FEDERAL TRADE COMMISSION

Ms. PARNES. Thank you, Chairman Dorgan. I appreciate the opportunity to appear before you today to discuss the Commission's work on issues related to online behavioral advertising.

Balancing consumers' online privacy interests against the development of successful online business models has been a top priority for the Commission over the past decade. Behavioral advertising, the use of tracking data to target advertisements to online consumers, is a challenging issue. It may provide benefits to consumers in the form of advertising that is more relevant to their interests, as well as a reduction in unwanted ads. It may also help support a diverse range of free online content that consumers would otherwise have to pay for, for example, blogging, search engines, social networking, and instant access to newspapers from around the world.

At the same time, many consumers express discomfort about the privacy and data security implications of being tracked. Without adequate safeguards in place, consumer tracking data could fall into the wrong hands or be used for unanticipated purposes. These concerns are exacerbated when tracking involves, for example, sensitive information about children's health or a consumer's finances. Further, particular concerns have been raised about tracking done by network advertisers across many sites, and most recently we saw significant consumer concern when one ISP announced and then abandoned plans to track every move of its customers as they navigate online.

The FTC has examined behavioral advertising for more than a decade, almost since the Internet transformed into a commercial medium. Our most recent efforts began in November of 2006 when we held 3 days of public hearings on technology issues likely to affect consumers in the next decade. Following these hearings, Commission staff held a series of meetings with stakeholders to learn more about behavioral advertising, and in November 2007, the Commission hosted a town hall devoted exclusively to behavioral advertising.

Several key points emerged at the town hall.

First, participants confirmed that online behavioral advertising may provide valuable benefits to consumers.

Second, the invisibility of the practice to consumers raises privacy concerns, as does the risk that data collected for behavioral advertising could be misused.

And third, business and consumer groups alike expressed support for transparency and consumer control in the online marketplace.

In December 2007, following the town hall, Commission staff issued and requested comments on proposed principles for online behavioral advertising to spur continuing public dialogue and encourage meaningful self-regulation. In brief, the proposed principles identify four issues to consider in developing a self-regulatory scheme.

First, companies that collect information for behavioral advertising should provide meaningful disclosures to consumers about

the practice, as well as choice about whether their information is collected for this purpose.

Second, companies should provide reasonable security for behavioral data so that it does not fall into the wrong hands and should retain data only as long as necessary to fulfill a legitimate business or law enforcement need.

Third, before a company uses behavioral data in a manner that is materially different from promises made when the data was initially collected, it should obtain affirmative express consent from the consumer.

Fourth, companies should obtain affirmative express consent before they use sensitive data for behavioral advertising.

Commission staff received over 60 thoughtful, constructive, and diverse comments on the principles. The comment period has closed, and we are carefully evaluating the comments that we have received. Included in the comments were a number of specific proposals for how self-regulation could be implemented, as well as reports about steps taken to address privacy concerns since the town hall. Although there clearly is more work to be done, the Commission is cautiously optimistic that the privacy issues raised by online behavioral advertising can be effectively addressed through self-regulation. In such a dynamic and diverse environment, self-regulation may, indeed, be the best means to develop workable approaches to privacy.

The Commission, of course, will continue to monitor the marketplace to keep pace with developments, gain a better understanding of the issues, and take appropriate action to protect consumers as circumstances warrant.

Thank you for your attention, and I would, of course, be happy to answer any questions.

[The prepared statement of Ms. Parnes follows:]

PREPARED STATEMENT OF LYDIA B. PARNES, DIRECTOR,
BUREAU OF CONSUMER PROTECTION, FEDERAL TRADE COMMISSION

I. Introduction

Chairman Inouye, Vice Chairman Stevens, and Members of Committee, I am Lydia Parnes,[1] Director of the Bureau of Consumer Protection at the Federal Trade Commission (the "FTC" or "Commission"). I appreciate the opportunity to appear before you today to discuss the Commission's activities regarding online behavioral advertising, the practice of collecting information about an individual's online activities in order to serve advertisements that are tailored to that individual's interests. Over the past year or so, the Commission has undertaken a comprehensive effort to educate itself and the public about this practice and its implications for consumer privacy. This testimony will describe the Commission's efforts, which have included hosting a "Town Hall" meeting and issuing for public comment FTC staff's proposed online behavioral advertising principles.[2]

The Commission's examination of behavioral advertising has shown that the issues surrounding this practice are complex, that the business models are diverse and constantly evolving, and that behavioral advertising may provide benefits to consumers even as it raises concerns about consumer privacy. At this time, the

[1] The views expressed in this statement represent the views of the Commission. My oral presentation and responses to any questions are my own, however, and do not necessarily reflect the views of the Commission or any individual Commissioner.

[2] *See* Federal Trade Commission, "Ehavioral Advertising: Tracking, Targeting, and Technology," available at *http://www.ftc.gov/bcp/workshops/ehavioral/index.shtml*.

Commission is cautiously optimistic that the privacy concerns raised by behavioral advertising can be addressed effectively by industry self-regulation.[3]

II. Behavioral Advertising

Many businesses use online behavioral advertising in an attempt to increase the effectiveness of their advertising by targeting advertisements more closely to the interests of their audience. The practice generally involves the use of "cookies" to track consumers' activities online and associate those activities with a particular computer or device. In many cases, the information collected is not personally identifiable in the traditional sense—that is, the information does not include the consumer's name, physical address, or similar identifier that could be used to identify the consumer in the offline world. Many of the companies engaged in behavioral advertising are so-called "network advertisers," companies that serve advertisements across the Internet at websites that participate in their networks.[4]

An example of how behavioral advertising might work is as follows: a consumer visits a travel website and searches for airline flights to New York City. The consumer does not purchase any tickets, but later visits the website of a local newspaper to read about the Washington Nationals baseball team. While on the newspaper's website, the consumer receives an advertisement from an airline featuring flights to New York City.

In this simple example, the travel website where the consumer conducted his research might have an arrangement with a network advertiser to provide advertising to its visitors. The network advertiser places on the consumer's computer a cookie, which stores non-personally identifiable information such as the web pages the consumer has visited, the advertisements that the consumer has been shown, and how frequently each advertisement has been shown. Because the newspaper's website is also part of the advertising network, when the consumer visits the newspaper website, the network advertiser recognizes the cookie from the travel website as its own and identifies the consumer as likely having an interest in traveling to New York. It then serves the corresponding advertisement for airline flights to New York.

In a slightly more sophisticated example, the information about the content that the consumer had selected from the travel website could be combined with information about the consumer's activities on the newspaper's website. The advertisement served could then be tailored to the consumer's interest in, not just New York City, but also baseball (*e.g.,* an advertisement referring to the New York Yankees).

As these examples illustrate, behavioral advertising may provide benefits to consumers in the form of advertising that is more relevant to their interests. Consumer research has shown that many online consumers value more personalized ads, which may facilitate shopping for the specific products that consumers want.[5] Further, by providing advertisements that are likely to be of interest to the consumer, behavioral advertising also may reduce the number of unwanted, and potentially unwelcome, advertisements consumers receive online.

More broadly, the revenue model for the Internet is, to a large extent, advertising-based, and using behavioral techniques can increase the cost-effectiveness of online advertising. Thus, behavioral advertising may help subsidize and support a diverse range of free online content and services that otherwise might not be available or that consumers would otherwise have to pay for—content and services such as blogging, search engines, social networking, and instant access to newspapers and information from around the world.

At the same time, however, behavioral advertising raises consumer privacy concerns. As described below, many consumers express discomfort about the privacy implications of being tracked, as well as the specific harms that could result. In particular, without adequate safeguards in place, consumer tracking data may fall into

---

[3] Although FTC staff has proposed self-regulation to address the general privacy concerns raised by behavioral advertising, the Commission will of course continue to bring enforcement actions to challenge law violations in appropriate cases.

[4] The advertisements are typically based upon data collected about a given consumer as he or she travels across the different websites in the advertising network. A website may belong to multiple networks.

[5] *See* Larry Ponemon, "FTC Presentation on Cookies and Consumer Permissions," presented at the FTC's Town Hall "Ehavioral Advertising: Tracking, Targeting, and Technology" (Nov. 1, 2007), at 7, available at *http://www.ftc.gov/bcp/workshops/ehavioral/presentations/31ponemon.pdf* (survey found that 55 percent of respondents believed that an online ad that targeted their individual preferences or interests improved, to some degree, their online experience). *See also* TRUSTe/TNS Presentation, TRUSTe and TNS Global, "Consumer Attitudes about Behavioral Advertising" at 10 (March 28, 2008) (72 percent of respondents found online advertising annoying when it was not relevant to their interests or needs). *But see infra* note 13 and accompanying text.

the wrong hands or be used for unanticipated purposes.[6] These concerns are exacerbated when the tracking involves sensitive information about, for example, children, health, or a consumer's finances.

Recent high-profile incidents where tracking data has been released have magnified consumers' concerns. In August 2006, for example, an employee of Internet service provider and web services company AOL made public the search records of approximately 658,000 customers.[7] The search records were not identified by name, and, in fact, the company had taken steps to anonymize the data. By combining the highly particularized and often personal searches, however, several newspapers, including the *New York Times*,[8] and consumer groups were able to identify some individual AOL users and their queries, challenging traditional notions about what data is or is not personally identifiable.

Another incident involved the social networking site Facebook. In November 2007, Facebook released a program called Beacon, which allowed users to share information about their online activities, such as the purchases they had made or the videos they had viewed. The Beacon service tracked the activities of logged-in users on websites that had partnered with Facebook. If a user did not opt out of this tracking, Facebook's partner sites would send to Facebook information about the user's purchases at the partner sites. Facebook then published this information on the user's profile page and sent it to the user's Facebook "friends."

The Beacon program raised significant concerns among Facebook users.[9] Approximately 30 groups formed on Facebook to protest Beacon, with one of the groups representing over 4,700 members,[10] and over 50,000 Facebook users signed a petition objecting to the new program.[11] Within a few weeks, Facebook changed its program by adding more user controls over what information is shared with "friends" and by improving notifications to users before sharing their information with others on Facebook.[12]

Surveys confirm that consumers are concerned about the privacy of their activities as they navigate online. For example, in two recent surveys, a majority of consumers expressed some degree of discomfort with having information about their online activities collected and used to serve advertising.[13] Similarly, only 20 percent of consumers in a third survey stated that they would allow a marketer to share information about them in order to track their purchasing behaviors and to help predict future purchasing decisions.[14] Another survey found that 45 percent of consumers believe that online tracking should be banned, and another 47 percent would

---

[6] As a result of these concerns, a number of consumer groups and others have asked the Commission to take action in this area. *See, e.g.,* Center for Digital Democracy and U.S. Public Interest Research Group Complaint and Request for Inquiry and Injunctive Relief Concerning Unfair and Deceptive Online Marketing Practices (Nov. 1, 2006), available at *http://www.democraticmedia.org/files/pdf/FTCadprivacy.pdf;* Ari Schwartz and Alissa Cooper, Center for Democracy and Technology, "CDT Letter to Commissioner Rosch," (Jan. 19, 2007), available at *http://www.cdt.org/privacy/20070119rosch-behavioral-letter.pdf*; Mindy Bockstein, "Letter to Chairman Majoras Re: DoubleClick, Inc. and Google, Inc. Merger," New York State Consumer Protection Board (May 1, 2007), available at *http://epic.org/privacy/ftc/google/cpb.pdf.*

[7] *See, e.g.,* Jeremy Kirk, "AOL Search Data Reportedly Released," *Computerworld* (Aug. 6, 2007), available at *http://computerworld.com/action/article.do?command=viewArticleBasic&taxonomyName=privacy&articleId=9002234&taxonomyId=84.*

[8] *See* Michael Barbaro and Tom Zeller, "A Face Is Exposed for AOL Searcher No. 4417749," *www.nytimes.com,* Aug. 9, 2006, available at *http://www.nytimes.com/2006/08/09/technology/09aol.html*.

[9] In one now-famous example, a man had bought a ring for his wife as a surprise; the surprise was ruined when his wife read about his purchase on the man's user profile page. *See, e.g.,* Ellen Nakashima, "Feeling Betrayed, Facebook Users Force Site to Honor Privacy," *Washingtonpost.com,* (Nov. 30, 2007), available at *http://www.washingtonpost.com/wp-dyn/content/article/2007/11/29/AR2007112902503_pf.html.*

[10] *See* Facebook home page, *http://www.facebook.com,* viewed on March 21, 2008.

[11] MoveOn.org Civic Action™ created an online petition for consumers to express their objection to Facebook's Beacon program. The petition stated, "Sites like Facebook must respect my privacy. They should not tell my friends what I buy on other sites—or let companies use my name to endorse their products—without my explicit permission." MoveOn.org Civic Action Petition, available at *http://www.civic.moveon.org/facebookprivacy/*, viewed June 9, 2008.

[12] *See* Reuters News, "Facebook Makes Tweak After Privacy Protest," *RedHerring.com,* Nov. 30, 2007, available at *http://www.redherring.com/Home/23224.*

[13] *See* Alan Westin, "Online Users, Behavioral Marketing and Privacy: Results of a National Harris/Westin Survey" (March 2008) (almost 60 percent of respondents were "not comfortable" to some degree with online behavioral marketing); TRUSTe/TNS Presentation, "Behavioral Advertising: Privacy, Consumer Attitudes and Best Practices," at 10 (April 23, 2008) (57 percent of respondents were not comfortable with advertisers using browsing history to serve ads, even if the information is not connected to personally identifiable information).

[14] *See* Ponemon Presentation, *supra* note 5, at 11.

allow such tracking, but only with some form of consumer control.[15] These surveys underscore the importance of online privacy to consumers and highlight the fundamental importance of maintaining trust in the online marketplace.

III. FTC Initiatives Concerning Consumer Privacy and Behavioral Advertising

Since privacy first emerged as a significant consumer protection issue in the mid-1990s, it has been one of the Commission's highest priorities. The Commission has worked to address privacy issues through consumer and business education, law enforcement, and policy initiatives. For example, the FTC has promulgated and enforced the Do Not Call Rule to respond to consumer complaints about unsolicited and unwanted telemarketing;[16] has waged a multi-faceted war on identity theft;[17] has encouraged better data security practices by businesses through educational initiatives[18] and a robust enforcement program;[19] has brought numerous enforcement actions to reduce the incidence of spun and spyware;[20] and has held numerous workshops to examine emerging technologies and business practices, and the privacy and other issues they raise for consumers.[21] In early 2006, recognizing the ever-increasing importance of privacy to consumers and to a healthy marketplace, the Commission established the Division of Privacy and Identity Protection, a division devoted exclusively to privacy-related issues.

In developing and implementing its privacy program, the FTC has been mindful of the need for flexibility and balance—that is, the need to address consumer concerns and harms without stifling innovation or imposing needless costs on consumers and businesses.

A. 1999 Workshop on Online Profiling

The Commission first examined the issue of behavioral advertising in 1999, when it held a joint public workshop with the Department of Commerce on the practice—then called "online profiling." The workshop examined the practice of tracking consumers' activities online, as well as the role of self-regulation in this area.

---

[15] *See* George R. Milne, "Information Exchange Expectations of Consumers, Marketing Managers and Direct Marketers," University of Massachusetts Amherst (presented on Nov. 1, 2007), available at *http://www.ftc.gov/bcp/workshops/ehavioral/presentations/3gmilne.pdf*.

[16] Telemarketing Sales Rule: Final Rule, 16 C.F.R. Part 310 (2003), available at *http://www.ftc.gov/os/2003/01/tsrfrn.pdf*.

[17] *See, e.g.*, FTC ID theft website, available at *www.ftc.gov/idtheft*. In one recent effort, the FTC coordinated with the U.S. Postal Service to send a letter to every American household containing information about how to protect against identity theft. *See* Press Release, "Postmaster General Sends Advice to Prevent ID Theft," U.S. Postal Service (Feb. 19, 2008), available at *http://www.usps.com/connnunications/newsroom/2008/pr08_014.htm*.

[18] *See, e.g.,* Federal Trade Commission, "Protecting Personal Information: A Guide for Business," available at *http://www.ftc.gov/infosecurity/; see also http://onguardonline.gov/index.html*.

[19] Since 2001, the Commission has obtained twenty consent orders against companies that allegedly failed to provide reasonable protections for sensitive consumer information. *See In the Matter of The TJX Companies,* FTC File No. 072–3055 (Mar. 27, 2008, settlement accepted for public comment); *In the Matter of Reed Elsevier Inc. and Seisint Inc.,* FTC File No. 052–3094 (Mar. 27, 2008, settlement accepted for public comment); *United States* v. *ValueClick, Inc.,* No. CV08–01711 (C.D. Cal. Mar. 13, 2008); *In the Matter of Goal Financial, LLC,* FTC Docket No. C–4216 (April 15, 2008); *In the Matter of Life is Good, Inc.,* FTC Docket No. C–4218 (Apr. 18, 2008); *United States* v. *American United Mortgage,* No. CV07C 7064, (N.D. Ill. Dec. 18, 2007); *In the Matter of Guidance Software, Inc.,* FTC Docket No. C–4187 (Apr. 3, 2007); *In the Matter of CardSystems Solutions, Inc.,* FTC Docket No. C–4168 (Sept. 5, 2006); *In the Matter of Nations Title Agency, Inc.,* FTC Docket No. C–4161 (June 19, 2006); *In the Matter of DSW, Inc.,* FTC Docket No. C–4157 (Mar. 7, 2006); *United States* v. *ChoicePoint, Inc.,* No. 106–CV–0198 (N.D. Ga. Feb. 15, 2006); *In the Matter of Superior Mortgage Corp.,* FTC Docket No. C–4153 (Dec. 14, 2005); *In the Matter of BJ's Wholesale Club, Inc.,* FTC Docket No. C–4148 (Sept. 20, 2005); *In the Matter of Nationwide Mortgage Group, Inc.,* FTC Docket No. 9319 (Apr. 12, 2005); *In the Matter of Petco Animal Supplies, Inc.,* FTC Docket No. C–4133 (Mar. 4, 2005); *In the Matter of Sunbelt Lending Services,* FTC Docket No. C–4129 (Jan. 3, 2005); *In the Matter of MTS Inc., d/b/a Tower Records/Books/Video,* FTC Docket No. C–4110 (May 28, 2004); *In the Matter of Guess?, Inc.,* FTC Docket No. C–4091 (July 30, 2003); *In the Matter of Microsoft Corp.,* FTC Docket No. C–4069 (Dec. 20, 2002); *In the Matter of Eli Lilly & Co.*, FTC Docket No. C–4047 (May 8, 2002).

[20] Since 2004, the Commission has initiated eleven spyware-related law enforcement actions. Detailed information regarding each of these law enforcement actions is available at *http://www.ftc.gov/bcp/edu/microsites/spyware/law_enfor.htm.* Since 1997, when the FTC brought its first enforcement action targeting unsolicited commercial e-mail, or "spam," the FTC has brought 94 law enforcement actions. *See generally* Report on "Spam Summit: The Next Generation of Threats and Solutions" (Nov. 2007), available at *http://www.ftc.gov/os/2007/12/071220spamsummitreport.pdf*.

[21] *See* discussion *infra* pp. 9–12.

In response to the concerns highlighted at the workshop, industry members formed the Network Advertising Initiative ("NAI"), a self-regulatory organization addressing behavioral advertising by network advertisers. Shortly thereafter, the NAI issued the NAI Self-Regulatory Principles ("NAI Principles") governing collection of information for online advertising by network advertisers.[22] In the early 2000s, however, with the "burst" of the dot com bubble, many network advertisers—including most of the NAI membership—went out of business.

Emblematic of the highly dynamic nature of the online environment, by the time the FTC held its public hearings on Protecting Consumers in the Next Tech-ade ("Tech-ade") only a few years later,[23] the issue of online tracking and advertising had reemerged. In the intervening years, behavioral advertising had become a highly successful business practice, and a number of Tech-ade participants raised concerns about its effects on consumer privacy.

B. The FTC Town Hall on Online Behavioral Advertising

Beginning in Fall 2006, the Commission staff held a series of meetings with numerous industry representatives, technology experts, consumer and privacy advocates, and academics to learn more about the practice of behavioral advertising. The purpose of these meetings was to explore further the issues raised at Tech-ade, learn about developments since the FTC's 1999 Workshop, and examine concerns about behavioral advertising that had been raised by privacy advocates and others.[24] Seeking a broader forum in which to examine and discuss these issues, and particularly the privacy issues raised by the practice, the FTC held a two-day Town Hall meeting on behavioral advertising in November 2007.

From the Town Hall, as well as the meetings preceding it, several key points emerged. First, as discussed above, online behavioral advertising may provide many valuable benefits to consumers in the form of free content, personalization that many consumers value, and a potential reduction in unwanted advertising. Second, the invisibility of the practice to consumers raises privacy concerns, as does the risk that data collected for behavioral advertising—including sensitive data about children, health, or finances—could be misused. Third, business and consumer groups alike expressed support for transparency and consumer control in the online marketplace.

Many participants at the Town Hall also criticized the self-regulatory efforts that had been implemented to date. In particular, these participants stated that the NAI Principles had not been sufficiently effective in addressing the privacy concerns raised by behavioral advertising because of the NAP s limited membership, the limited scope of the NAI Principles (which apply to network advertisers but not to other companies engaged in behavioral advertising), and the NAI Principles' lack of enforcement and cumbersome opt-out system.[25] Further, while other industry associations had promulgated online self-regulatory schemes to address privacy issues, these schemes had not generally focused on behavioral advertising.[26]

---

[22] Briefly, the NAI Principles set forth guidelines for online network advertisers and provide a means by which consumers can opt out of behavioral advertising at a centralized website. For more information on the FTC workshop and NAI, *see Online Profiling: A Report to Congress* (June 2000) at 22 and *Online Profiling: A Report Congress Part 2 Recommendations* (July 2000), available at *http://www.ftc.gov/os/2000/06/onlineprofilingreportjune2000.pdf* and *http://www.networkadvertising.org*. As discussed further below, NAI recently proposed for public comment revised NAI Principles.

[23] The purpose of the Tech-ade hearings, held in November 2006, was to examine the technological and consumer protection developments anticipated over the next decade. *See generally http://www.ftc.gov/bcp/workshops/techade/index.html*.

[24] *See* CDD *et al.,* Complaint and Request for Inquiry and Injunctive Relief, *supra* note 6. Many of these concerns were amplified by the announcement of the proposed merger between Google and DoubleClick in April 2007. The Commission approved the merger on December 20, 2007, at the same time that it issued FTC staff's proposed self-regulatory guidelines. *See* "Staff Proposes Online Behavioral Advertising Policy Principles," Federal Trade Commission (Dec. 20, 2008), available at *http://www.ftc.gov/opa/2007/12/principles.shtm.* The Principles are discussed *infra* at 13.

[25] According to critics, the NAI Principles' opt-out mechanism is difficult to locate and use because it is located on the NAI website, where consumers would be unlikely to find it. As noted above, in April of this year, the NAI issued a proposed revised set of self-regulatory principles designed to address criticisms of the original NAI Principles and to respond to the FTC staff's call for stronger self-regulation. The NAI has sought comment on its proposed revised principles, and comments were due June 12, 2008. *See* "Self-Regulatory Principles for Online Preference Marketing By Network Advertisers," Network Advertising Initiative (issued April 10, 2008), available at *http://www.networkadvertising.org/pdfs/NAI_principles.pdf.*

[26] Since the Town Hall, some of these industry groups, as well as several online companies and privacy groups, have sought to address the concerns raised about behavioral advertising.

Continued

C. The FTC's Proposed Self-Regulatory Principles

In December 2007, in response to the issues discussed at the Town Hall and in public comments received in connection with that event, Commission staff issued and requested comment on a set of proposed principles titled, "Behavioral Advertising: Moving the Discussion Forward to Possible Self-Regulatory Principles" (the "Principles"). The proposed Principles address the central concerns about online behavioral advertising expressed by interested parties; they also build upon existing "best practices" in the area of privacy, as well as (in some cases) previous FTC guidance and/or law enforcement actions. At the same time, the Principles reflect FTC staff's recognition of the potential benefits provided by online behavioral advertising and the need to maintain vigorous competition in this area.

The purpose of the proposed Principles is to encourage more meaningful and enforceable self-regulation. At this time, the Commission believes that self-regulation may be the preferable approach for this dynamic marketplace because it affords the flexibility that is needed as business models continue to evolve.

In brief, the staff proposal identifies four governing principles for behavioral advertising.[27] The first is transparency and consumer control: companies that collect information for behavioral advertising should provide meaningful disclosures to consumers about the practices, as well as choice about whether their information is collected for this purpose.[28] The second principle is reasonable security: companies should provide reasonable security for behavioral data so that it does not fall into the wrong hands, and should retain data only as long as necessary to fulfill a legitimate business or law enforcement need.[29] The third principle governs material changes to privacy policies: before a company uses behavioral data in a manner that is materially different from promises made when the data was collected, it should obtain affirmative express consent from the consumer.[30] This principle ensures that consumers can rely on promises made about how their information will be used, and can prevent contrary uses if they so choose. The fourth principle states that companies should obtain affirmative express consent before they use sensitive data—for example, data about children, health, or finances—for behavioral advertising.[31]

IV. Next Steps

In response to the request for public comment, Commission staff received over 60 comments on the Principles, representing many thoughtful and constructive views from diverse business sectors, industry self-regulatory bodies, privacy advocates, technologists, academics, and consumers. The comment period for the Principles has closed, and Commission staff is carefully evaluating the comments received.

Included in the comments were a number of specific proposals for how self-regulation could be implemented, as well as reports regarding steps taken to address privacy concerns since the Town Hall. The FTC is encouraged by the efforts that have

---

See, e.g., Interactive Advertising Bureau, "Privacy Principles," (adopted Feb. 24, 2008), available at *http://www.iab net/iab_products_and_industry_services/1421/1443/1464;* Comment "Online Behavioral Advertising: Moving the Discussion Forward to Possible Self-Regulatory Principles," Microsoft Corp. (April 11, 2008), available at *http://www.ftc.gov/os/comments/behavioraladprinciples/080411microsoft.pdf;* Comment "FTC Staff Proposed Online Behavioral Advertising Principles: Comments of AOL, LLC," AOL, LLC (April 11, 2008), available at *http://www.ftc.gov/os/comments/behavioraladprinciples/080411aol.pdf;* Ari Schwartz, Center for Democracy and Technology, *et al.,* "Consumer Rights and Protections in the Behavioral Advertising Sector," (Oct. 31, 2007) (proposing a "Do Not Track List" designed to increase consumers' control over tracking of their activities online), available at *http://www.cdt.org/privacy/20071031consumerprotectionsbehavioral.pdf.*

[27] Recent news reports have highlighted concerns about behavioral advertising involving Internet Service Providers ("ISPs"). The ISP-based model for delivering behaviorally-targeted advertising may raise heightened privacy concerns because it could involve the tracking of subscribers wherever they go online and the accumulation of vast stores of data about their online activities. Further, information about the subscriber's activities potentially could be combined with the personally identifiable information that ISPs possess about their subscribers. In issuing the proposed Principles for public comment, FTC staff intended the Principles to apply to ISPs.

[28] For more information and guidance on the use of disclosures in online advertising, *see Dot Com Disclosures, Information About Online Advertising, http://www.ftc.gov/bcp/conline/pubs/buspubs/dotcom/index.shtml* (May 2000).

[29] The FTC has highlighted the need for reasonable security in numerous educational materials and enforcement actions to date. *See supra* notes 18–19.

[30] *See, e.g., Gateway Learning Corp.,* Docket No. C–4120 (Sept. 10, 2004), *http://www.ftc.gov/opa/2004/07/gateway.shtm* (company made material changes to its privacy policy and allegedly applied such changes to data collected under the old policy; opt-in consent required for future such changes).

[31] Commission staff also sought comment on the potential uses of tracking data beyond behavioral advertising.

already been made by the NAI[32] and some other organizations and companies[33] and believes that the self-regulatory process that has been initiated is a promising one. Although there is more work to be done in this area, the Commission is cautiously optimistic that the privacy issues raised by online behavioral advertising can be effectively addressed through meaningful, enforceable self-regulation. The dynamic and diverse online environment demands workable and adaptable approaches to privacy that will be responsive to the evolving marketplace. Nevertheless, the Commission will continue to closely monitor the marketplace so that it can take appropriate action to protect consumers as the circumstances warrant.

V. Conclusion

The Commission appreciates this opportunity to discuss its work on behavioral advertising. The Commission is committed to addressing new and emerging privacy issues such as online behavioral advertising and looks forward to working further with the Committee on this important consumer issue.

Senator DORGAN. Ms. Parnes, thank you very much.

Next we will hear from Ms. Jane Horvath, the Senior Privacy Counsel at Google, Incorporated. Ms. Horvath?

STATEMENT OF JANE HORVATH, SENIOR PRIVACY COUNSEL, GOOGLE, INC.

Ms. HORVATH. Senator Dorgan and Senator Vitter, the most important point I would like to make this morning is simple. Google makes privacy a priority because our business depends on it. If our users are uncomfortable with how we manage their personal information, they are only one click away from switching to a competitor's services.

Putting our users first means that we are deeply committed to their privacy, and succeeding in online advertising and protecting our users' privacy are not mutually exclusive goals.

This morning I will first discuss how online advertising benefits advertisers, website publishers, and Internet users. Second, I will discuss Google's approach to privacy. And finally, I will make recommendations for how government and industry can better protect Internet users' privacy.

So let me first touch on the benefits of online advertising. Google's two primary advertising programs, AdWords and AdSense, provide users with highly relevant ads, match advertisers with users who are interested in their products, and provide revenue for website publishers who place our ads on their sites. For example, in Minneapolis, taxi driver Kenny Kormendy, built a website for out-of-state travelers called Gopher State Taxi and used Google's AdWords program to compete online with bigger taxi companies. Today Gopher State Taxi has grown to a network of over 36 cabs, and Mr. Kormendy credits Google with connecting 9 out of 10 of its customers.

When someone clicks on one of our ads on a website, Google also shares revenue from that ad with the website owner. Last year we paid a total of $4.5 billion in ad revenue to website publishers across the United States.

---

[32] Current NAI members include DoubleClick, Yahoo! Inc., TACODA, Inc., Acerno, AlmondNet, BlueLithium, Mindset Media, Revenue Science, Inc., 24/7 Real Media Inc., and Undertone Networks.

[33] *See supra* note 26. Although many organizations and consumer groups have undertaken efforts to address FTC staff's proposed Principles, a few organizations have expressed concern that implementing the Principles would be too costly and would undermine continued development of the online marketplace. FTC staff is evaluating all of these comments as it considers next steps in this area.

Next, let me talk about Google's approach to privacy. As I said earlier, Google makes privacy a priority because our business depends on it. We make sure that three design fundamentals are the bedrock of our privacy practices.

First, transparency. We have been an industry leader in finding new ways to educate users about privacy such as through our Google Privacy Channel on YouTube where we feature videos that explain our privacy policies in plain language.

Second, choice. We strive to design our products in a way that gives users meaningful choices about what information they provide to us. For example, our Google Talk instant messaging service includes an "off the record" feature that prevents either party from storing the chat.

And third, security. We take seriously the protection of data that our users entrust with us. Google employs some of the world's best engineers in software and network security and has teams dedicated to developing information safeguards. Google's advertising products are primarily driven by context rather than behavior. Unlike other companies we have built our business on showing ads that are relevant to what a user is looking for, not by building detailed profiles based on a user's online behavior.

As we continue to incorporate DoubleClick's display ad serving capabilities into our business, Google will continue to be a leader in offering products that respect privacy.

Finally, let me turn to our efforts to innovate in the area of privacy protection. Feedback from our users and outside parties, as well as our own internal discussions, has led us to several privacy innovations, including our decision last year to anonymize our server logs after 18 months. In that spirit of innovation today, we offer the following recommendations for both government and the private sector.

First, Google supports the passage of a comprehensive Federal privacy law that will establish a uniform framework for privacy and put penalties in place to punish and dissuade bad actors.

Second, we support the Federal Trade Commission's efforts to develop principles relating to online privacy and behavioral advertising, and we hope that revised principles will be adopted widely by the online ad industry.

And third, we believe that greater labeling of online display ads should be adopted as an industry standard.

As I conclude my testimony this morning and welcome the Committee's questions, I would like to show a brief excerpt from one of the videos on our Google Privacy YouTube Channel. This video shows a user how to easily remove cookies from their web browsers. Thank you.

[Video shown.]

[The prepared statement of Ms. Horvath follows:]

PREPARED STATEMENT OF JANE HORVATH, SENIOR PRIVACY COUNSEL, GOOGLE, INC.

Chairman Inouye, Vice Chairman Stevens, Members of the Committee.

I'm pleased to appear before you this morning to discuss online advertising and the ways that Google protects our users' privacy. My name is Jane Horvath, and I am Google's Senior Privacy Counsel. In that role I am responsible for working with

our product teams and other privacy professionals at Google to ensure compliance with privacy laws and develop best practices for protecting our users' privacy.

Google's mission is to organize the world's information and make it universally accessible and useful. The best known way that we do this today is through our search engine, which is available for free to Internet users throughout the world. The availability of Google search and our other products—and the improvements that we make to our products on a daily basis—is funded by online advertising, by far our primary source of revenue.

Online advertising is relatively young and a very small piece of the advertising market as a whole. It is a dynamic business characterized by strong competition, significant innovation, and continuing growth. Online advertising has succeeded because it helps businesses find customers more efficiently and effectively than through other media. It has also helped to create entirely new and innovative small businesses that generate revenue through advertising, often in partnership with Google.

At Google we believe that our online advertising business has succeeded because our most important advertising goal is to deliver ads that benefit our users. From its inception, Google has focused on providing the best user experience possible. We do this, for example, by ensuring that advertising on our site delivers relevant content that is not a distraction. In fact, our goal is to make our ads just as useful to Google's users as search results themselves.

We've also made a commitment to never compromise the integrity of our search results, for example by manipulating rankings to place our partners higher in our search results. And advertising on Google is always clearly identified as a "Sponsored Link" to ensure that our users know the difference between our search results and any advertising that we provide.

Putting our users first also means that we are deeply committed to their privacy, and our products and policies demonstrate that commitment. We believe that success in online advertising and protecting our users' privacy are not mutually exclusive goals. We work hard to provide advertising in a way that is transparent to users, provides them with appropriate choices, and protects any personal information that we collect from inappropriate access by third parties.

In my testimony this morning, I would like to cover three key points:

First, I'll explain Google's main advertising products and the significant benefits that we at Google believe online advertising brings to advertisers, online publishers, and individual Internet users.

Second, I'll discuss Google's approach to privacy, specific steps that we take to protect our users' privacy, and privacy issues involving our advertising business.

And finally, I'll explore ideas and make recommendations for how to better protect Internet users' privacy both with respect to advertising as well as more generally as more and more information moves to the Internet cloud.

The Benefits of Online Advertising

Google offers three main advertising products: AdWords, AdSense for Search, and AdSense for Content. Our AdWords product allows us to provide ads on Google.com in response to search queries entered by our users, as well as to provide ads on our AdSense for Content and AdSense for Search services. AdSense for Search allows us to provide ads in response to search queries entered by users of our partners' search engines, including AOL and *Ask.com.* AdSense for Content allows us to provide ads to visitors of our third-party publisher partners' websites. AdSense for Content ads are provided based on the content of the page that is being viewed by a user. The vast majority of the revenue that Google generates comes from these three products.

All three advertising products are primarily easy-to-create text ads, which is one of the many reasons that hundreds of thousands of small businesses advertise with us. We also provide the capability to show display ads—ads that incorporate graphics in addition to text—through AdSense for Content, and we plan to enhance our display ad serving capabilities with our recent acquisition of DoubleClick, a display ad serving technology company.

Advertisers, online publishers, and consumers all benefit from our advertising network. I'll start with consumers—our users—on whom our business depends.

In our experience, users value the advertisements that we deliver along with search results and other web content because the ads help connect them to the information, products, and services they seek. The ads we deliver to our users complement the natural search results that we provide because our users are often searching for products and services that our advertisers offer. Making this connec-

tion is critical, and we strive to deliver the ads that are the most relevant to our users, not just the ones that generate the most revenue for us. We do this through our innovative ad auction system, which gives weight to the relevancy—the usefulness—of the ad to our users based on their search queries or the content that they are viewing. And in our pay-per-click pricing model we only generate revenue when a user is interested enough to click on an ad.

The revenue that we generate from online advertising makes it possible for Google to offer dozens of free products to our users—everything from search and e-mail to our word processing application, Google Docs. Each of these products underscores our commitment to improving our users' online experience. For example, Google Docs allows multiple users to edit a single document, presentation, or spreadsheet at the same time. And, despite the popularity of tools like Google Earth and YouTube, each of our products is free to individuals for personal use. Our online advertising business model subsidizes the creation, development, and ongoing improvements to and support for these and future products.

And our ads aren't always commercial. We run a program called Google Grants that provides free advertising to not-for-profit organizations engaged in areas such as science and technology, education, global public health, the environment, youth advocacy, and the arts. For example, we have provided Google Grants to non-profits such as Room to Read (*www.roomtoread.org*), which educates children in Vietnam, Nepal, India, and Cambodia, and CoachArt (*www.coachart.org*), which provides therapeutic art and athletic lessons to underprivileged children with life-threatening illnesses. Since April 2003, our grantees have collectively received almost $300 million in free advertising.

Our advertising network also enables small businesses to connect with consumers that they otherwise would not reach, and to do so affordably, efficiently, and effectively. The advertiser decides the maximum amount of money it wishes to spend on advertising and, as noted above, in the cost-per-click payment model the advertiser only pays Google when a user actually clicks on an ad.

Here are just two of many stories of small businesses succeeding thanks to Google advertising. Suzanne Golter owns the Happy Hound dog daycare (*www.happyhound.com*) in Oakland, California. She estimates that 90 percent of her business is generated through Google AdWords, which helps her bring in approximately 40 new clients per month. In Minneapolis, Minnesota, Kenny Kormendy, a then-struggling taxi driver built a site for out-of-state travelers called Gopher State Taxi (*www.gopherstatetaxi.com*) and utilized AdWords to compete online with bigger taxi companies. In under 3 years, Gopher State Taxi has grown to a network of over 36 cabs, and Mr. Kormendy credits AdWords with connecting nine out of ten customers that his company services.

Online advertising also promotes freer, more robust, and more diverse speech. It's no coincidence that blogs have proliferated over the past few years. Our AdSense product enables bloggers and other publishers to generate revenue from ads that we place on their websites. Without online advertising, the individuals who run these sites would not be able to dedicate as much time and attention to their publications as they do today. In fact, we know that many website owners can afford to dedicate themselves to their sites full time because of online advertising.

AdSense revenues support hundreds of thousands of diverse websites, and a significant percentage of the revenue we earn from advertising ends up in the hands of the bloggers and website operators who partner with us by featuring ads provided by Google. Last year we paid $4.5 billion in advertising revenue from our AdSense program to our publishing partners. In Nevada, Arizona, Florida, and Washington alone over 100,000 of our publishing partners collectively generated nearly $100 million from AdSense in 2007.

The vast majority of these AdSense partners are small businesses. For example, in Oregon, Hope Pryor, a grandmother of four, uses AdSense on her site—*Cooksrecipes.com*—to generate her primary source of income. And in Massachusetts, honey bee aficionado and retiree Albert Needham uses AdSense revenue generated from his *Bees-online.com* website to fund personal vacations. Similar small business success stories are found all across the United States.

It's no mistake that I've focused mainly on individual users, small publishers, and small advertisers. Google's business model has concentrated on what's known as the "long tail" of the Internet—the millions of individuals and small businesses that cater to and need to connect with niche interests and markets. Google's advertising programs lower the barrier to entry for small publishers and advertisers alike, and connect them with users who are interested in what they have to say or sell. As our advertising business continues to grow and evolve, we will continue working hard to encourage the development of the long tail.

Google and Privacy

We believe user trust is essential to building the best possible products. With every Google product, we work hard to earn and keep that trust with a long-standing commitment to protect the privacy of our users' personal information. We make privacy a priority because our business depends on it. In fact, if our users are uncomfortable with how we manage their personal information, they are only one click away from switching to a competitor's services.

Because user trust is so critical to us, we've ensured that privacy considerations are deeply embedded in our culture. Though I am Google's Senior Privacy Counsel, I am just one of many individuals at Google who work on privacy. For example, we have product counsels who work with engineers and product managers from the beginning of product development to ensure that our products protect our users' privacy. We also have product managers dedicated to privacy and other trust and safety issues. And we have a Privacy Council, which is comprised of a cross-functional group of Google employees that convenes on a regular basis to help Google address privacy issues.

Google's focus on user trust and privacy means that our product teams are thinking about user privacy by building privacy protections into our products from the ground up. For example, we have designed most of our products to allow people to use them anonymously, and to ensure that none of our products use any personally identifiable data unless that use is fully disclosed in our privacy policy.

We have also made sure that three design fundamentals—all of them rooted in fair information principles—are at the bedrock of our privacy products and practices:

- *Transparency:* We believe in being upfront with our users about what information we collect and how we use it so that they can make informed choices about their personal information. We have been an industry leader in finding new ways to educate users about privacy, such as through our Google Privacy Channel on YouTube (found at *www.youtube.com/googleprivacy*) where we feature privacy videos that explain our privacy policies, practices, and product features in simple, plain language.
- *Choice:* We strive to design our products in a way that gives users meaningful choices about how they use our services and what information they provide to us. Many of our products, including our Search service, do not require users to provide any personally identifying information at all. When we do ask for personal information, we also endeavor to provide features that give users control over that information. For example, our Google Talk instant messaging service includes an "off the record" feature that prevents either party from storing the chat.
- *Security:* We take seriously the protection of data that our users entrust with us. Google employs some of the world's best engineers in software and network security and has teams dedicated to developing and implementing policies, practices and technologies to protect this information. More information about our approach to security can be found in a recent post at the Official Google Blog located at *googleblog.blogspot.com/2008/03/how-google-keeps-your-information.html*.

One of our newest products is Google Health, which enables individuals to consolidate and store their medical records and personal health information online. Google Health demonstrates our commitment to all three design fundamentals. For example, we have provided significant transparency about Google Health's privacy features through blog posts and the product's easy-to-understand privacy policy and frequently asked questions. In addition, Google Health provides users choice by empowering them with the decision of what information to import, share, and delete, and easy tools for accomplishing each.

The online advertising products that we offer today are also privacy-friendly because they are primarily contextual in nature. That is, we generally provide ads in response to what a user is searching for or viewing at the time, rather than based on who we believe the user may be or an extended history of the user's activities either online or off.

To respond to our users' desire for more relevant advertising, and to advertisers' desire to provide more relevant advertising to Internet users, we are experimenting with some forms of online advertising that do involve more than the current search query to provide an ad. For example, we are currently experimenting in Google.com search with providing ads based on both the current query and a previous search. A user who types "Italy vacation" into the Google search box, for instance, might see ads about Tuscany or affordable flights to Rome. If the user were to subse-

quently search for "weather," we might assume that there is a link between "Italy vacation" and "weather" and deliver ads regarding local weather conditions in Italy. However, Google does not build a profile of the user to serve these ads that is stored and used later to serve other ads to the user.

As we continue to incorporate DoubleClick into our business, our focus on display advertising—ads that feature images in addition to text—will increase across our advertising product offerings, as will our ability to provide metrics and an improved user experience to our AdSense network. We believe that expanding into display advertising products is one way that we can compete effectively in the highly competitive online advertising environment. This transition will not undermine Google's focus on privacy or our commitment to the fundamental principles of transparency, choice, and security. As we move to offer more display advertising and other advertising products, Google intends to continue to be a leader in offering products that protect and respect the privacy of our users.

Google's Efforts to Continue Innovating in Privacy

In our quickly evolving business environment, ensuring that we earn and keep our users' trust is an essential constant for building the best possible products. With every Google product, we work hard to earn and keep that trust with a long-standing commitment to protect the privacy of our users' personal information. As stated above, the bedrock of our privacy practices are three design fundamentals: transparency, choice, and security.

Another constant that we have found in our business is that innovation is a critical part of our approach to privacy. To best innovate in privacy, we welcome the feedback of privacy advocates, government experts, our users, and other stakeholders. This feedback, and our own internal discussions about how to protect privacy, has led us to several privacy innovations including our decision last year to anonymize our server logs after 18 months.

In the interest of continuing to protect individuals' privacy, we offer the following policy and technology recommendations—some of which can be accomplished by the private sector and some of which involve a government role—in the spirit of continuing the effort to innovate on consumer privacy. Our ideas and recommendations endorse a baseline and robust level of privacy protections for all individuals. On top of that baseline platform we believe that the private sector and government should cooperate to educate and inform consumers about privacy issues and to establish best practices that will help guide the development of the quickly evolving and innovative online advertising space. Finally, we believe that Google and others in the online advertising industry should work to provide tools to better protect individuals' privacy, and that government should encourage companies to experiment with new and innovative ways of protecting consumers' privacy.

Comprehensive Federal Privacy Law

Google supports the passage of a comprehensive Federal privacy law that would accomplish several goals such as building consumer trust and protections; establishing a uniform framework for privacy, which would create consistent levels of privacy from one jurisdiction to another; and putting penalties in place to punish and dissuade bad actors. We believe that as information flows increase and more and more information is processed and stored in the Internet cloud—on remote servers rather than on users' home computers—there is a greater need for uniform data safeguarding standards, data breach notification procedures, and stronger procedural protections relating to government and third party litigant access to individuals' information.

Behavioral Advertising Principles

We have participated actively in the Federal Trade Commission's efforts to develop privacy principles relating to online privacy and behavioral advertising. Our hope is that revised principles will be adopted widely by the online advertising industry and serve as a model for industry self-regulation in jurisdictions beyond the United States. In order for the principles to achieve such broad adoption, however, they need to be revised to ensure that they can be operationalized by industry and that they will give consumers appropriate transparency, choice, and security. In order for that to happen, the principles would, among other things, need to make a distinction between personally identifiable information (PII) and non-PII.

Consumer Education

Transparency is one of Google's bedrock design principles because we believe that informed and knowledgeable users are best able to protect their privacy. We believe that both the private sector and the government, including agencies like the FTC, can and should provide more information about what kinds of personal information

are collected by companies, how such data is used, and what steps consumers can take to better protect their privacy.

At Google, for example, we take great pride in our effort to provide our users with a better understanding of how we collect, use, and protect their data through a series of short videos available at Google.com and on YouTube, as well as through blog posts. Too often, website operators view their online privacy policy—which is typically impenetrable to the average user—as the beginning and end of their privacy obligations. Web companies that interact with individuals need to do more than simply provide and link to privacy policies; we need to offer consumer-friendly materials in different media to better help their users understand how their information is collected and used, and what choices they have to protect their privacy.

Transparency and Choice in Display Advertising

Google text ads are generally labeled "Ads by Google" or "Sponsored Links" and are accompanied by an explanation of what they are so that users understand that they are advertisements and that they have been provided by Google. We believe that this kind of notice and explanation should be adopted by industry and applied not only to text ads but also to display ads. We also believe that industry should continue working together to provide, for example, effective mechanisms that empower consumers with the ability to opt out of behaviorally targeted advertising.

Development of Technology to Empower Users

Products like Google Toolbar let a user choose to not have data collected, and that choice persists even if all cookies are cleared and until the user chooses to have data collected. Google also offers features like Web History, which allows users to view and search all search queries they have made on Google search while logged into Google. Web History also lets users delete and thus disassociate from their account information any searches that they conduct while they are logged in. Users can also pause Web History altogether if they do not want their searches to be associated with their account information—and this choice persists until users choose to resume Web History. We believe that more can be done by industry to ensure the persistence of users' choices, and we look forward to exploring such tools with industry and other stakeholders.

Conclusion

Chairman Inouye, Vice Chairman Stevens, and Members of the Committee, thank you for the opportunity to testify today. I appreciate the opportunity to explain the benefits of our advertising business to consumers, advertisers, and publishers, and the chance to explain how Google protects our users' privacy.

I look forward to answering any questions you might have about our efforts, and Google looks forward to working with Members of the Committee and others in the development of better privacy protections for Internet users everywhere.

Thank you.

Senator DORGAN. Ms. Horvath, does that complete your testimony?

Ms. HORVATH. Yes. Thank you very much.

Senator DORGAN. Ms. Horvath, thank you very much.

Next we will hear from Mr. Robert Dykes, who is the Chairman and CEO of NebuAd, Incorporated. Mr. Dykes, welcome. You may proceed.

STATEMENT OF ROBERT R. DYKES, FOUNDER, CHAIRMAN, AND CEO, NEBUAD, INC.

Mr. DYKES. Thank you, Chairman Dorgan and Senator Vitter. My name is Bob Dykes, CEO of NebuAd, Inc., a recent entrant into the online advertising industry that partners with Internet service providers, otherwise known as ISP's. I come from a security background, serving for many years as Executive Vice President of Symantec Corporation.

When we launched NebuAd several years ago, it was at a time when many people had particularly heightened concerns about data security. As part of its mission, NebuAd sought to address these

privacy and security concerns. As you will see, NebuAd systems are designed so that no one, not even the government, can determine the identity of our users.

Currently online advertising solutions and data collection methods operate in many locations throughout the Internet ecosystem, from users' computers to individual websites, to networks of websites. The NebuAd service, in partnership with ISP's, provides consumers with significant benefits serving them with more relevant ads which they want, while ensuring that they have robust privacy protections and control over their online experience.

NebuAd's ad network also is designed to benefit two groups that provide substantial benefit to the Internet: many smaller websites and general use sites that have difficulty maintaining free access to their content; the ISP's who need to upgrade their infrastructure to provide increased bandwidth for consumers who increasingly want access to Internet delivered videos. NebuAd creates these benefits by using a select set of a user's Internet activities to construct anonymous inferences about likely interests which are then used to select and serve the most relevant advertisements.

The NebuAd service is architected and its operations are based on principles essential to strong privacy protection. We provide users with prior robust notice about the service and opportunity to express informed choice about whether to participate both before the service takes effect and persistently thereafter. We do not collect or use personally identifiable information, or PII. We do not store raw data linked to identifiable individuals, and we provide state-of-the-art security for the limited amount of information we do store. In other words, allegations by others that we do not provide an opportunity to opt out in our robust notice to users or that we collect entire web traffic of users are simply not accurate.

To repeat, NebuAd provides robust notice and the opportunity to express informed choice, and there is no collection or use of any personally identifiable information or even a significant portion of users' web traffic, nor any information from password-protected sites, web mail, e-mail, instant messages, or VoIP traffic.

We understand that to gain the public's trust, we need to adopt strong privacy protections. Ours have been reviewed by such entities as the Ponemon Institute, and we are engaging a Big Four audit firm to conduct an audit to verify that we do what we say we do.

This Committee has long been involved with the creation of privacy statutes covering the cable and telecommunications industries, as well as specific statutes addressing online privacy for children, telemarketing, and spam. Yet even though these and other privacy statutes have been developed one at a time, there are common threads running through them all. When more sensitive data is collected and when the collection and disclosure of the data could harm or embarrass a consumer, more rigorous disclosure and consent requirements tend to be imposed. When raw data linked to an identifiable individual is stored for longer periods, there is an emerging trend that more rigorous disclosure, consent, and security requirements should be imposed.

NebuAd supports the privacy paradigm which provides users with consistent expectations and substantial protections. This para-

digm also is technology- and business-neutral, and it is the basis upon which NebuAd built its technology and operations. NebuAd urges the Committee to maintain both the paradigm and the principle of technology and business neutrality.

Thank you.

[The prepared statement of Mr. Dykes follows:]

PREPARED STATEMENT OF BOB DYKES, CEO, NEBUAD, INC.

Chairman Inouye, Ranking Member Stevens, and Members of the Committee, thank you for inviting me to appear today regarding the privacy implications of online advertising. My name is Bob Dykes, CEO of NebuAd, Inc., a recent entrant into the online advertising industry that partners with Internet Service Providers (ISPs). I have spent considerable time over the past year with Federal policymakers at the Federal Trade Commission (FTC), Federal Communications Commission, and in Congress—as well as with consumer and privacy advocates—discussing NebuAd's technology, operations, and privacy protections and welcome the opportunity to discuss all of this further with the Committee.

Introduction

Online advertising is a phenomenon of the Internet age. It permits advertisers to provide more relevant messages to consumers and in turn fuels the development of website publishers, both large and small. In fact, advertising is the engine for the free Internet. The FTC has found online advertising benefits consumers by enabling "access to newspapers and information around the world, provided free because it is subsidized by online advertising; tailored ads that facilitate comparison shopping for the specific products that consumers want; and, potentially, a reduction in ads that are irrelevant to consumers' interests and that may therefore be unwelcome." [1]

Within this world of online advertising, NebuAd is a newcomer, just entering among industry giants like Google, Yahoo!, Microsoft, Amazon, and countless website publishers. That means we have a steep hill to climb, but it also means we have great opportunities. We are able to learn the lessons of the industry and construct state-of-the-art technology that delivers ads that are more relevant to users while providing them with robust and industry-leading privacy protections. Indeed, as I will discuss, these privacy protections are built into our technology and designed into our policies from the ground up.

Let me explain our privacy motivation more fully. I come from a security background, serving for many years as Executive Vice President of Symantec Corporation, a global leader in providing security solutions for computers and computer networks. When we launched NebuAd several years ago, it was at a time when many people had particularly heightened concerns about data security. Hackers were piercing firewalls, seeking to capture seemingly random strands of data to find the identity of users. The government was ordering ISPs and other network providers to turn over data on their users. As part of its mission, NebuAd sought to address these privacy and security concerns.

The NebuAd service is architected and its operations are based on principles essential to strong privacy protection:

- Provide users with prior, robust notice and the opportunity to express informed choice about whether to participate, both before the service takes effect and persistently thereafter;
- Do not collect or use personally-identifiable information ("PII");
- Do not store raw data linked to identifiable individuals; and
- Provide state-of-the art security for any information stored.

As a result, NebuAd's service is designed so that no one—not even the government—can determine the identity of our users. That means our service for ISP users, including the ad optimization and serving system, does not collect or use any PII. In addition, NebuAd requires its Internet service provider ("ISP") partners to

[1] It is an axiom that advertising has more value when the advertiser believes the user is more interested in the advertiser's product. Such interest is not obvious when a user visits general-purpose news and information sites, which are some of the very ones noted by the FTC Staff as standing to benefit from online advertising. Accordingly, the online advertising industry is constantly seeking other ways to infer user interest and then bring that knowledge to bear on the placement of ads on these sites. That is, behavioral advertising drives value and supports those sites on the Internet that provide society with great value.

provide robust, advance notice about our operations and our privacy protections to their subscribers, who at any time can exercise their choice not to participate. And, finally, we have located our servers in highly secure data centers.

The NebuAd Technology and its Advertising Operations

Currently, online advertising solutions operate in many locations throughout the Internet ecosystem—from users' computers to individual websites to networks of websites. When an Internet user visits the sites of web publishers, like Yahoo! or Amazon, these sites typically collect information about the user's activities to target ads based on that information. When an Internet user conducts a search, the search company may collect information from the user's activity, which in turn may be used to improve the relevance of the ads shown. And when a user visits a website within an online advertising network, some of which include thousands of sites, the visits help the network advertising company categorize a user for targeted advertising. All of these activities are well-entrenched in the Internet and, given the enormous and growing use of the Internet, have proven to have mutual benefits for users, publishers—large and small—advertisers, and ad networks.

NebuAd provides online advertising in partnership with ISPs. The NebuAd advertising service has been architected to use only a select set of a user's Internet activities (only a subset of HTTP traffic) to construct anonymous inferences about the user's level of qualification for a predefined set of market segment categories ("anonymous user profiles"), which are then used to select and serve the most relevant advertisements to that user. The NebuAd advertising service does not collect or use any information from password-protected sites (*e.g.,* HTTPS traffic), web mail, e-mail, instant messages, or VoIP traffic. Using only non-PII, NebuAd constructs and continuously updates these unique and anonymous user profiles.[2]

In the course of these business operations, NebuAd's ad optimization and serving system does not collect PII or use information deemed to be sensitive (*e.g.,* information involving a user's financial, sensitive health, or medical matters).[3] In addition, NebuAd requires its ISP partners to provide robust disclosure notices to users prior to initiating any service and permits them to opt-out of having their data collected and receiving targeted ads. Once a user opts-out, NebuAd deletes that user's anonymous user profile and will ignore the user's subsequent web navigation activity.[4]

Finally, NebuAd's ad optimization and serving system operates similar to traditional ad networks. It makes standard use of cookies for accepted ad serving purposes. It makes standard use of pixel tags that operate only within the security framework of the browser to invoke the placement of ad network cookies and that contain no uniquely identifying number, subscriber identifier, or any other subscriber information. In sum, NebuAd's code used for standard ad serving purposes is both clean in its purpose and function.

The Privacy Paradigm in the United States and NebuAd's Privacy Protections

In contrast to the European Community, where omnibus privacy law covers all industries, in the United States, privacy statutes have been developed in a largely sector-specific fashion. This Committee has long been part of that trend, having overseen the creation of privacy statutes generally covering the cable and telecommunications industries, as well as specific statutes addressing online privacy for children, telemarketing, and spam. Yet, even though these and other privacy statutes have been developed one at a time, there are common threads running through them:

- When more sensitive data is collected, and when the collection and disclosure of the data could harm or embarrass a consumer, more rigorous disclosure and consent requirements tend to be imposed.

---

[2] The anonymous user profiles do not contain any original raw data, such as URLs navigated, but only consist of a set of numbers that represent the anonymous inferences about the user's level of qualification for a predefined set of market segment categories.

[3] NebuAd understands that the definition of "sensitive" information will evolve. We stated in our comments to the FTC on the "Staff's Proposed Principles for the Self-Regulation of Behavioral Advertising" that we would adopt the Staff's definition of "sensitive" information, assuming it is not limitless. We also would consider additional reasonable limitations proposed by other stakeholders.

[4] NebuAd has enhanced the industry-standard opt-out "cookie" based system with the use of proprietary techniques. This enables the opt-out to be more persistent. NebuAd's entire enhanced opt-out system is linked to individual computers and browsers, and it informs users of this fact in assisting them in understanding the nature of their opt-out choice.

- When raw data linked to an identifiable individual is stored for longer periods, there is an emerging trend that more rigorous disclosure, consent, and security requirements should be imposed.

NebuAd supports this privacy paradigm, which provides users with consistent expectations and substantial protections. This paradigm also is technology and business-neutral, and it is the basis upon which NebuAd built its technology and operations. NebuAd urges the Committee to maintain both the paradigm and the principle of technology and business-neutrality.

In implementing this privacy paradigm, NebuAd not only relied on the expertise of its own personnel, it turned to leading privacy experts, including Fran Maier, Executive Director and President of TRUSTe, the consumer privacy organization, Dr. Larry Ponemon of the Ponemon Institute, and Alan Chapell of Chapell & Associates. These experts provided important input into NebuAd's initial privacy program. They were particularly stringent in recommending that NebuAd should not collect PH or sensitive information and that it provide consumers with robust notice and choice. NebuAd followed that guidance in developing our privacy program.[5]

The following are the key privacy protections upon which NebuAd has architected into its technology and based its operations:

1. *NebuAd's service does not collect or use PII from ISP subscribers.* The entire ad optimization and serving system does not collect or use any PII, nor does it collect any information from password-protected sites, web mail, e-mail, instant messages, or VoIP traffic.

2. *NebuAd stores only a set of numbers that represent the user's level of qualification for a predefined set of market segment categories ("anonymous user profiles").* NebuAd does not store raw data such as URLs navigated or IP addresses associated with an identifiable individual. Rather, the NebuAd service constructs anonymous inferences about the user's level of qualification for a predefined set of market segment categories, and then discards the raw data that was used to create or update a user's anonymous profile. This mechanism of constructing anonymous inferences about the user's level of qualification and not storing raw data provides a strong additional layer of privacy protection that goes beyond the standards used by many Internet companies today.

3. *NebuAd's ISP Partners are required to provide robust, direct notice in advance of launch of the service.* The notice discloses to the user that the ISP is working to ensure that advertisements shown will be more relevant advertisements, that to deliver these ads its partner creates anonymous profiles based on part of the user's web-surfing behavior, which does not include the collection of PII, and that the user may opt-out of the service. For existing subscribers, the notice is required to be delivered 30 days prior to the launch of the service by postal mail, e-mail, or both.[6] For new subscribers, the notice is required to be placed clearly and conspicuously in the new subscriber sign-up flow and outside the privacy policy. All subscribers can opt-out at any time, and ongoing disclosure and opportunity to opt-out is required to be provided within the ISP's privacy policy.

4. *NebuAd and its ISP partners offer users advance and on-going choice of opting-out of the service.* Users are provided with a clear statement of what opt-out means and the way it operates. Once the opt-out option is chosen, NebuAd honors that choice and ignores the user's subsequent web surfing activity and thus does not serve the user with behaviorally targeted ads.[7]

5. *NebuAd's service only creates anonymous user profiles, which contain no PII and no raw data, and its placement of ads is completely anonymous.* NebuAd uses proprietary algorithms and techniques, including one-way encryption of data, so that no one—not even NebuAd's engineers who designed the system—can reverse-engineer an anonymous identifier, or the anonymous user profile associated with it, to an identifiable individual.

---

[5] A just released survey of U.S. Internet users by TRUSTe showed that 71 percent of online consumers are aware their web-surfing information may be collected for the purpose of advertising and 91 percent wanted to have the tools to assure they could protect their privacy. NebuAd has strived to provide users with this transparency by educating users about its activities and their choices regarding whether to participate in NebuAd's services.

[6] NebuAd seeks to ensure that users are fully informed of its activities and are given full opportunity to choose whether to participate. To that end, we are developing enhanced notification mechanisms.

[7] The user, of course, will continue to receive ads.

6. *NebuAd avoids any sensitive websites or product categories.* NebuAd does not track or serve ads based on visits related to adult content, sensitive medical information, racial or ethnic origins, religious beliefs or content of a sexual nature, and does not have market segment categories for illegal products.

7. *NebuAd does not permit either complexity of data or narrowness of data to be reverse-engineered into PII.* This protection is accomplished because anonymous user profiles are constructed by anonymous inferences about the consumer's level of qualification for a predefined set of market segment categories. Raw data is simply not stored as part of the anonymous user profile. In addition, the NebuAd service does not have narrowly-defined segments. Finally, the anonymous profile identifier is the result of multiple encryptions, and based on multiple data elements including the hashed IP address.

8. *There is no connection or link between the ISP's registration data systems and NebuAd.* That means that no user-specific data is exchanged between NebuAd and ISP data systems. This boundary is preserved further and inadvertent disclosure is prevented because NebuAd immediately performs a one-way encryption of the IP address and other anonymous user identifiers used within the NebuAd system.

9. *NebuAd installs no applications on users' computers, has no access to users' hard drives, and has no access to secure transactions.* As such, NebuAd does not control a user's computer or web-surfing activity in any way (*e.g.,* by changing computer settings or observing private or sensitive information).

10. *NebuAd's Data Centers are professionally operated and secured.* NebuAd's servers are located at secure sites with state-of-the-art protections against any intrusion, electronic or physical.

NebuAd is proud of these protections—all of which were adopted to comply with both the spirit and letter of the government's privacy paradigm—and, it continuously seeks to enhance them.

Conclusion

As I stated at the outset, I have spent years seeking to ensure that users have robust and transparent privacy protections. In a very real sense, NebuAd is the product of that work—It has adopted and implemented state-of-the-art privacy protections, and, equally as important, it has established a process to continuously improve on them. The Internet is a highly dynamic environment, where new technologies are constantly developed to address new challenges, and we both want and need to take advantage of them. NebuAd takes its responsibilities to its users very seriously. It looks forward to continuing to work with government policymakers as they examine online advertising and privacy issues.

Senator DORGAN. Mr. Dykes, thank you very much. We appreciate your being here.

Next we will hear from Ms. Leslie Harris, who is the President and Chief Executive Officer of the Center for Democracy and Technology. Ms. Harris, you may proceed.

STATEMENT OF LESLIE HARRIS, PRESIDENT AND CEO, CENTER FOR DEMOCRACY AND TECHNOLOGY

Ms. HARRIS. Thank you. Chairman Dorgan, Members of the Committee, I thank you for the opportunity testify today.

I want to make three points and offer several recommendations for the Committee.

First, while behavioral advertising is growing, consumers are largely uncomfortable with the practice and they are ill-equipped to take meaningful steps to protect their privacy. We do recognize that advertising is an important engine of Internet growth and that ad revenue supports a rich diversity of online content. However, massive increases in data processing and storage have allowed advertisers to track, collect, and aggregate information about consumers' web browsing across sites over time and to compile individual profiles, and while each piece of consumer information in a

profile may itself not be personally identifiable, the aggregation of this information into rich profiles means it may be more readily tied to a person's identity.

All this is happening in an environment where more data is being collected, retained for longer periods of time, often in a form where it can be re-identified. Existing privacy protections are outstripped by technology and there is a lack of transparency about behavioral advertising practices and an absence of meaningful controls to help consumers make informed decisions about the use of their data.

When consumers do find out about behavioral advertising, they are uncomfortable. In a recent study, 59 percent of the respondents said they were not comfortable with online companies using their browsing behavior to target advertising to their interests even when they were told that advertising supports free services.

Second, there is an emerging behavioral advertising model that partners ISPs with ad networks, and this does add new legal complexity and additional risks for privacy. While online websites and networks can track what you see on their sites or the sites associated with their networks, an ISP model may—and I do say "may"—provide access to everything you do online. And that would include noncommercial sites that could reveal political preferences, charitable, religious associations, and the like.

Consumers simply do not have an expectation that their web traffic is being intercepted by their ISP and shared with an unknown third party for profiling. And in our view, the law does not permit it. We read the Wiretap Act which prohibits interception and disclosure of electronic communications, including the content of Internet traffic, to require unavoidable notice and affirmative express consent for ISP-based behavioral targeting. And many state communications laws require two-party consent, which further complicates the legal landscape. And of course, the Cable Communications Policy Act also prohibits the collection or disclosure of personal information without prior consent.

The implementation that we have seen thus far completely fails to acknowledge, let alone comply with, these laws. No one has sought consent.

Finally, self-regulation is not a full answer. CDT has always been supportive of self-regulation, but the Network Advertising Initiative that was launched 8 years ago has been largely a failure. The model fell short when it was announced. It has failed to evolve over time. And only now when the FTC has turned its attention to the issues has the Initiative proposed modest improvements.

We acknowledge that there are a number of individual companies that have worked hard to educate and improve their users' privacy. We are prepared to continue to work with them and the NAI to continue to improve privacy protection.

Self-regulation was never expected to be a full solution. And when the NAI was created, the FTC at that point noted that backstop legislation would still be required to ensure consumers' privacy is protected.

We have made a number of recommendations for Committee action in our written testimony. Let me just briefly highlight a few.

First, Senator Dorgan, we agree with you that more hearings are necessary on the ISP question and on other questions like sensitive information and secondary use.

Second, we really urge this Committee to set a goal of enacting general privacy legislation in the next year based on well-established fair information practices. We have been advocating for this for years. We think it is time to act.

Third, we do think the FTC should issue its guidelines. We think they need to be enforceable whether they are under current authority or under targeted legislation. We think the Committee should make that clear to the FTC.

And finally, we think Congress should encourage the FTC to investigate how technological solutions, including perhaps a "Do Not Track" regime—we were part of a group that proposed that—can give consumers better control over their online information.

We do think Congress has a critical role to play in ensuring privacy protection in this increasingly complex online advertising environment, and I look forward to answering your questions.

[The prepared statement of Ms. Harris follows:]

PREPARED STATEMENT OF LESLIE HARRIS, PRESIDENT/CEO, CENTER FOR DEMOCRACY AND TECHNOLOGY

Chairman Inouye and Members of the Committee:

On behalf of the Center for Democracy and Technology ("CDT"), I thank you for the opportunity to testify today. We applaud the Committee's leadership in examining the privacy impact of new online advertising models.

I. Summary

CDT recognizes that advertising is an important engine of Internet growth. Consumers benefit from a rich diversity of content, services and applications that are provided without charge and supported by advertising revenue. However, as sophisticated new behavioral advertising models are deployed, it is vital that consumer privacy be protected. Massive increases in data processing and storage capabilities have allowed advertisers to track, collect and aggregate information about consumers' web browsing activities, compiling individual profiles used to match advertisements to consumers' interests. All of this is happening in the context of an online environment where more data is collected—and retained for longer periods—than ever before and existing privacy protections have been far outpaced by technological innovation.

Behavioral advertising represents a small but rapidly growing part of the online advertising market. Market research firm eMarketer reported last year that spending on behaviorally targeted online advertising is expected to reach $1 billion this year and to quadruple by 2011.[1] The recent spate of acquisitions of the online advertising industry's largest players by major Internet companies is powerful evidence that the online advertising marketplace is headed toward more data aggregation tied to a single profile—and one that may be more readily tied to a person's identity.[2] And while we have yet to see evidence that this new advertising model will reap the promised rewards, it is already migrating from individual websites to the infrastructure of the Internet itself: In the last year, Internet Service Providers ("ISPs") have begun to form partnerships with ad networks to mine information from individual web data streams for behavioral advertising. Ad networks that partner with ISPs could potentially collect and record every aspect of a consumer's web browsing, including every web page visited, the content of those pages, how long

[1] "Behavioral Advertising on Target . . . to Explode Online," *eMarketer* (Jun. 2007), *http://www.emarketer.com/Article.aspx?id=1004989.*

[2] No fewer than five major mergers and acquisitions have been completed in the last 18 months: Google purchased online advertising company DoubleClick, Inc.; WPP Group, a large ad agency, acquired the online ad company 24/7 Real Media; Yahoo! acquired ad firm RightMedia; Microsoft acquired online ad service provider aQuantive; AOL purchased Tacoda, a pioneering firm in the area of behavioral advertising.

each page is viewed, and what links are clicked. E-mails, chats, file transfers and many other kinds of data could all be collected and recorded.

The ISP model raises particularly serious questions. Thus far, implementations appear to defy reasonable consumer expectations, could interfere with Internet functionality, and may violate communications privacy laws.

Notwithstanding the recent growth of behavioral advertising, most Internet users today do not know that their browsing information may be tracked, aggregated and sold. After almost a decade of self-regulation, there is still a profound lack of transparency associated with these practices and an absence of meaningful consumer controls.

There are several efforts underway to respond to the new online advertising environment. First, the Federal Trade Commission staff recently released a draft of proposed principles for self-regulation, which represent a solid step forward. However, it is not clear whether the FTC will formally adopt the principles or put its enforcement power behind them.

The Network Advertising Initiative ("NAI") is also in the process of revising its guidelines. This is a welcome but long-overdue development. Unfortunately, self-regulation has not worked to date and, even if strengthened, will never by itself fully protect consumers' privacy interests.

Congress needs to take a comprehensive look at the current and emerging practices associated with behavioral advertising and the risks those practices pose to consumer privacy and control. We recommend that Congress take the following steps to address the significant privacy concerns raised by behavioral advertising:

- The Committee should hold a series of hearings to examine specific aspects of behavioral advertising, in particular the growing involvement of ISPs, the use of sensitive information, and secondary uses of behavioral profiles.
- The Committee should set a goal of enacting in the next year a simple, flexible baseline consumer privacy law that would protect consumers from inappropriate collection and misuse of their personal information, both online and offline.
- The Committee should strongly urge the Federal Trade Commission to exercise its full enforcement authority over online advertising practices.
- Congress should examine and strengthen existing communications privacy laws to cover new services, technologies and business models with consistent rules. The Electronic Communications Privacy Act ("ECPA") is decades old, and its application in today's online world is often unclear.
- Congress should encourage the FTC to investigate how technology can be harnessed to give consumers better control over their online information. Simple tools that put consumers in controls of their information, such as a "Do Not Track" list, deserve consideration.

II. Understanding Online Advertising Practices

Commercial websites that supply content to consumers free of charge are often supported by online advertising. These sites—known as "publishers" in the advertising world—make available certain portions of space on their pages to display ads. That space is sold to advertisers, ad agencies, or online ad intermediaries that find and place advertisements into the space. These intermediaries may also make arrangements to collect information about user visits to the publisher pages. Since very few publishers supply their own advertising, it is common that when a consumer visits a publisher site, the consumer's computer also connects to one or more advertisers, ad agencies, or ad intermediaries to send data about the consumer's visit to the site and receive the advertising on the site.

One type of ad intermediary is known as an "advertising network." At their most basic level, ad networks contract with many different publishers on one side and many different advertisers on the other. Armed with a pool of space in which to display ads on publisher sites, and a pool of ads to display, ad networks are in the business of matching up the two by using the data they collect about consumers' site visits.

A. Contextual Advertising

There are many different ways for an ad network to determine which advertisement should be placed in which space. The two most often discussed are "contextual" advertising and "behavioral" advertising. Contextual advertising, which is often used to generate ads alongside search results, matches advertisements to the content of the page that a consumer is currently viewing—a consumer who visits a sports site may see advertisements for golf clubs or baseball tickets on that site.

The privacy risks associated with contextual advertising vary. If the practice is transparent to the user and data collection and retention is minimal, the practice

poses little risk. By contrast, privacy concerns are heightened if the user data is retained in an identifiable or pseudonymous form (*i.e.,* linked to a user identifier) for long periods of time even if it is not immediately used to create advertising profiles.

B. Behavioral Advertising

By contrast, behavioral advertising matches advertisements to the interests of the consumer as determined over time. If a consumer visits several different travel sites before viewing a news site, he or she might see a behaviorally targeted travel advertisement displayed on the news page, even if the news page contains no travel content. A traditional behavioral ad network builds up profiles of individual consumers by tracking their activities on publisher sites in the network (although this model is evolving, as we discuss below). When the consumer visits a site where the ad network has purchased ad space, the ad network collects data about that visit and serves an advertisement based on the consumer's profile. Diagrams illustrating this process are included in Appendix A.

Consumers' behavioral advertising profiles may incorporate many different kinds of data that are in and of themselves not personally identifiable. Many networks avoid linking profiles to what has traditionally been considered "personally identifiable information" ("PII"): names, addresses, telephone numbers, e-mail addresses, and other identifiers. But as the comprehensiveness of consumer advertising profiles increases, the ability of marketers and others to link specific individuals to profiles is also growing. In 2006, for example, AOL released 3 months' worth of search queries generated by half a million users; in the interest of preserving users' anonymity, AOL replaced individuals' screen names with numbers. Based solely on search terms associated with one number, reporters at *The New York Times* were able to pinpoint the identity of the user who generated them.[3] The risk of supposedly non-personally identifying data being used to identify individuals has spurred several ad networks to take extra steps to de-identify or remove personal information from their data storage.[4]

Profiles may also be intentionally tied to PII. For example, data collected online by a merchant or by a service provider may permit an advertising profile to be tied to an individual's e-mail account. Offline data may also be merged with online profiles. For years, data service companies have maintained profiles about consumers based on information gleaned from public sources such as property and motor vehicle records, as well as records from sources like catalog sales and magazine subscriptions. These data companies are now also entering the online advertising business, potentially allowing the linking of online and offline profiles.[5]

C. The Evolution of Behavioral Advertising—More Data, More Data Sources

As noted above, recent market consolidation facilitates more comprehensive data collection. Companies that run consumers' favorite web-based services—web search, web mail, maps, calendars, office applications, and social networks—have all purchased behavioral advertising networks within the last year. In the past, major Internet companies could gather information about how an individual used its services and applications such as search, but did not have direct access to information about the user's other web browsing habits. With the acquisition of behavioral advertising networks, these companies could potentially marry the rich data about an individual's use of one site with a broad view of his or her activities across the web. The concerns about this aggregation of consumer data are heightened because many online companies retain data for months or years on end in identifiable or pseudonymous form, creating a host of privacy risks.

Finally, ad networks are now turning to the most comprehensive and concentrated source of information about Internet use: the individual web data streams that flow through ISPs.[6] In this emerging model, the ISP intercepts or allows an ad network

---

[3] Michael Barbaro and Tom Zeller, Jr., "A Face Is Exposed for AOL Searcher No. 4417749," *The New York Times* (Aug. 2006), *http://www.nytimes.com/2006/08/09/technology/ 09aol.html?_r=1&ex=1312776000&adxnnl=1&oref=slogin&adxnnlx=1215021816 2Dj7kbrLxHU1hCdcMyNqHEbA.*

[4] See, *e.g.,* Microsoft, *Privacy Protections in Microsoft's Ad Serving System and the Process of "De-identification"* (Oct. 2007), *http://download.microsoft.com/download/3/1/d/31df6942-ed99-4024-a0e0-594b9d27a31a/Privacy%20Protections%20in%20Microsoft%27s%20Ad%20serving%20system%20 and%20the%20Process%20of%20De-Identification.pdf.*

[5] Acxiom runs Relevance-X, an online ad network. Last year Experian acquired the online data analysis company Hitwise. *See* Acxiom, *Acxiom: Relevance-X* (last visited Jul. 2008), *http://www.acxiom.com/Relevance-X;* Experian, "Acquisition of Hitwise" (Apr. 2007), *http://www.experiangroup.com/corporate/ news/releases/2007/2007-904-17b/.*

[6] *See, e.g.,* Peter Whoriskey, "Every Click You Make," *The Washington Post* (Apr. 2008), *http://www.washingtonpost.com/wp-dyn/content/article/2008/04/03/AR2008040304052.html?nav=hcmodule;* Saul Hansell, "I.S.P. Tracking: The Mother of All Privacy Battles," *The New*

to intercept the content of each individual's web data stream. The ad network then uses this traffic data for behavioral advertising, serving targeted ads to the ISP's customers on publisher sites as the customers surf the web. We address the unique issues posed by this advertising model in detail below.

III. The Privacy Risks of Behavioral Advertising

Behavioral advertising poses a growing risk to consumer privacy; consumers are largely unaware of the practice and are thus ill equipped to take protective action. They have no expectation that their browsing information may be tracked and sold, and they are rarely provided sufficient information about the practices of advertisers or others in the advertising value chain to gauge the privacy risks and make meaningful decisions about whether and how their information may be used. In a recently released Harris Interactive/Alan F. Westin study, 59 percent of respondents said they were not comfortable with online companies using their browsing behavior to tailor ads and content to their interests even when they were told that such advertising supports free services.[7] A recent TRUSTe survey produced similar results.[8] It is highly unlikely that these respondents understood that this type of ad targeting is already taking place online every day.

In most cases, data collection for behavioral advertising operates on an opt-out basis. Opt-out mechanisms for online advertising are often buried in fine print, difficult to understand, hard to execute and technically inadequate. Only the most sophisticated and technically savvy consumers are likely to be able to successfully negotiate such opt-out processes. Moreover, in most cases, opt-out mechanisms offered for behavioral advertising only opt the user out of receiving targeted ads, but do not opt the user out of data collection about his or her Internet usage.

For behavioral advertising to operate in a truly privacy-protective way, data collection needs to be limited and data retention limits should be tied to the original purposes for collecting the data. Consumers need to be informed about what data is being collected about their Internet activities, how the information will be used, whether the information will be shared with others, and what measures are being taken to ensure that any transfer of data remains secure. They should be presented with this information in a manner that supports informed choice over their information and that choice should be honored persistently over time. Consumers must also have opportunities for legal redress for misuse of the data. As a recent D.C. District Court opinion established, data leakage and the concern for potential abuses of that data are recognizable harms standing alone, without any need to show misuse of the data.[9] Consumers do not need to become victims of identity theft to suffer from an invasion of privacy.

There is also a risk that profiles for behavioral advertising may be used for purposes other than advertising. For example, ad networks that focus on "re-targeting" ads may already be using profiles to help marketers engage in differential pricing.[10] Behavioral profiles, particularly those that can be tied to an individual, may also be a tempting source of information in making decisions about credit, insurance, and employment. While the lack of transparency makes it almost impossible to know whether behavioral profiles are being used for other purposes, the lack of enforceable rules around the collection and use of most personal information leaves the door wide open for a myriad of secondary uses.

Finally, because the legal standards for government access to personal information held by third parties are extraordinarily low, these comprehensive consumer

---

York Times: Bits Blog (Mar. 2008) at *http://bits.blogs.nytimes.com/2008/03/20/isp-tracking-the-mother-of-all-privacy-battles/?scp =1-b&sq=the+mother+of+all+privacy+battles&st=nyt.*

[7] Alan F. Westin, *How Online Users Feel About Behavioral Marketing and How Adoption of Privacy and Security Policies Could Affect Their Feelings* (Mar. 2008).

[8] TRUSTe, "TRUSTe Report Reveals Consumer Awareness and Attitudes About Behavioral Targeting" (Mar. 2008), *http://www.marketwire.com/mw/release.do?id=837437&sourceType=1* ("71 percent of online consumers are aware that their browsing information may be collected by a third party for advertising purposes. . . . 57 percent of respondents say they are not comfortable with advertisers using that browsing history to serve relevant ads, even when that information cannot be tied to their names or any other personal information.").

[9] *Am. Fed'n of Gov't Employees* v. *Hawley,* D.D.C., No. 07–00855, 3/31/08 (ruling, *inter alia,* that concerns about identity theft, embarrassment, inconvenience, and damage to financial suitability requirements after an apparent data breach constituted a recognizable "adverse effect" under the Privacy Act, 5 U.S.C. § 552(a) (citing *Kreiger* v. *Dep't of Justice,* 529 F.Supp.2d 29, 53 (D.D.C. 2008)).

[10] *See* Louise Story, "Online Pitches Made Just For You," *The New York Times* (Mar. 2008), *http://www.nytimes.com/2008/03/06/business/media/06adco.html.*

profiles are available to government officials by mere subpoena, without notice to the individual or an opportunity for the individual to object.[11]

IV. The Use of Sensitive Information for Behavioral Advertising

The concerns about behavioral advertising practices are heightened because of the increasingly sensitive nature of the information that consumers are providing online in order to take advantage of new services and applications. Two data types of particular concern are health information and location information.

A. Personal Health Information—Increasingly Available Online

Personal health data is migrating online through an ever-expanding array of health information and search sites, online support groups, and personal health record sites. Federal privacy rules under the Health Information Portability and Accountability Act ("HIPAA") do not cover personal health information once it moves online and out of the control of HIPAA-covered entities. Once it is posted online, it may have no more legal protection than any other piece of consumer information. In addition, information provided by consumers that is not part of a "medical record"—such as search terms—may nevertheless reveal highly sensitive information. We do not know the full extent to which personal health data is being collected for behavioral advertising. We do know that the limits placed on its collection by the industry are inadequate and that there is an urgent need to develop a definition for personal health information in the Internet context that is robust enough to protect privacy.

B. Location Information—Not Always Protected By Current Law

As technologies converge and Internet services are provided over cellular phones and other mobile devices, the ability to physically locate consumers is spurring location-based advertising, targeted to where a user is at any given moment. Plans to incorporate location information into behavioral advertising are still in development. Although laws exist to protect location information collected by telecommunications carriers, applications providers are increasingly offering location-based services that fall completely out of that legal framework. Standards for government access to location information are also unclear, even as law enforcement has shown a greater interest in such information.[12]

V. The Emerging Use of ISP Data for Behavioral Advertising

The use of ISP data for behavioral advertising is one area that requires close scrutiny from lawmakers. The interception and sharing of Internet traffic content for behavioral advertising defies reasonable user expectations, can be disruptive to Internet and Web functionality, and may run afoul of communications privacy laws.

A. How ISP Data is Used for Behavioral Advertising

In this new model, an ad network strikes a deal with an ISP that allows the network to receive the contents of the individual web traffic streams of each of the ISP's customers. The ad network analyzes the content of the traffic in order to create a record of the individual's online behaviors and interests. As customers of the ISP surf the Web and visit sites where the ad network has purchased ad space, they see advertisements targeted based on their previous Internet behavior. While the model as it exists today involves an ISP contracting with a third party that operates such an ad network, it would also be possible for ISPs to do the traffic content inspection, categorization, and advertising delivery themselves.

B. Privacy Implications of the Use of ISP Data for Behavioral Advertising

The privacy implications of behavioral advertising at large are amplified in this ISP model. Ad networks that partner with ISPs may potentially gain access to all or substantially all of an individual's Web traffic as it traverses the ISP's infrastructure, including traffic to all political, religious, and other non-commercial sites. While traditional ad networks may be large, few if any provide the opportunity to collect information about an individual's online activities as comprehensively as in the ISP model, particularly with respect to activities involving non-commercial con-

---

[11] *See* Center for Democracy and Technology, *Digital Search & Seizure: Updating Privacy Protections to Keep Pace with Technology* (2006), *http://www.cdt.org/publications/digital-search-and-seizure.pdf* at 7–9; Deirdre K. Mulligan, "Reasonable Expectations in Electronic Communications: A Critical Perspective on the Electronic Communications Privacy Act," 72 *Geo. Wash. L. Rev.* 1557 (Aug. 2004); Daniel J. Solove, "Digital Dossiers and the Dissipation of Fourth Amendment Privacy," 75 *S. Cal. L. Rev.* 1083, 1135 (2002).

[12] *See* Center for Democracy and Technology, *Digital Search & Seizure: Updating Privacy Protections to Keep Pace with Technology* (2006), *http://www.cdt.org/publications/digital-search-and-seizure.pdf* at 23–29.

tent. And although these ad networks currently inspect predominantly Web traffic, ISPs carry e-mails, chats, file transfers and many other kinds of data that they could decide to pass on to behavioral ad networks in the future.

Moreover, the use of Internet traffic content for behavioral advertising defies user expectations about what happens when they surf the Web and communicate online. Absent unmistakable notice, consumers simply do not expect their ISP or its partners to be looking into the content of their Internet communications. Finding out that there is a middleman lurking between consumers and the websites they visit would come as a unwelcome surprise to most Internet users. ISPs are a critical part of the chain of trust that undergirds the Internet. Giving an unknown third party broad access to all or most consumer communications may undermine that trust.

C. Current Implementations May Interfere With Normal Internet Use

Despite these concerns, several ad network companies are moving forward with plans to use ISP data for behavioral advertising. The two most prominent ad networks engaged in this practice are NebuAd in the United States and Phorm in the UK. Charter Communications, a cable broadband ISP, recently announced—and then delayed—a plan to conduct trials of the NebuAd behavioral advertising technology.[13] Several other ISPs, such as Wide Open West (WOW!), CenturyTel, Embarq and Knology also announced plans with NebuAd to trial or deploy its behavioral advertising technology. Although a number of these ISPs have put their plans on hold in the wake of a firestorm of criticism, NebuAd continues to work with U.S. ISPs and seek new ISP partners. Phorm, which originally announced deals with three of the UK's largest ISPs and has sought partnerships with U.S. ISPs, is also now encountering hesitation from some of its partners.[14]

Independent analyses of both companies' systems have revealed that by virtue of their ability to intercept Internet traffic in the middle of the network—and based on their desire to track individual Internet users—they engage in an array of practices that are inconsistent with the usual flow of Internet traffic. NebuAd reportedly injects computer code into Web traffic streams that causes numerous cookies to be placed on users' computers for behavioral tracking, none of which are related to or sanctioned by the websites the users visit.[15] When a user navigates to a particular website, Phorm reportedly pretends to be that website so that it can plant a behavioral tracking cookie linked to that site on the user's computer.[16] In addition to the privacy implications of tracking all of an individual's Web activities, this kind of conduct has the potential to create serious security vulnerabilities in the network,[17] hamper the speed of users' Internet connections, and interfere with ordinary Web functionality. At a time when many different kinds of companies are working to build a trusted computing platform for the Internet, having ISPs work with partners whose practices undermine trust raises future cyber-security concerns.

D. Current Implementations May Violate Federal Law

Depending on how this advertising model is implemented, it may also run afoul of existing communications privacy laws. The Federal Wiretap Act, as amended by the Electronic Communications Privacy Act ("ECPA"), prohibits the interception and disclosure of electronic communications—including Internet traffic content—without consent.[18] Although exceptions to this rule permit interception and disclosure without consent, we seriously doubt that any of them apply to the interception or disclosure of Internet traffic content for behavioral advertising purposes. Accordingly, we believe that the Wiretap Act requires unavoidable notice and affirmative opt-in consent before Internet traffic content may be used from ISPs for behavioral advertising purposes. Certain state laws may take this one step further, requiring consent from both parties to the communication: the consumer and the website he or she is visiting. A detailed CDT legal memorandum on the application of the Wiretap

---

[13] Saul Hansell, "Charter Suspends Plan to Sell Customer Data to Advertisers," *The New York Times: Bits Blog* (Jun. 2008), *http://bits.blogs.nytimes.com/2008/06/24/charter-suspends-plan-to-sell-customer-data-to-advertisers/?scp=3-b&sq=charter+nebuad&st=nyt.*

[14] Chris Williams, "CPW builds wall between customers and Phorm," *The Register* (Mar. 2008), *http://www.theregister.co.uk/2008/03/11/ phorm__shares__plummet/.*

[15] Robert M. Topolski, *NebuAd and Partner ISPs: Wiretapping, Forgery and Browser Hijacking,* Free Press and Public Knowledge (Jun. 2008), *http://www.publicknowledge.org/ pdf/ nebuad-report-20080618.pdf.*

[16] Richard Clayton, *The Phorm "Webwise"* System (May 2008), *http://www.cl.cam.ac.uk/rnc1/ 080518-phorm.pdf.*

[17] These types of behaviors have much in common with well-understood online security threats, and parts of the Internet security community are already investigating how to respond. *See* Anti-Spyware Coalition, "Anti-Spyware Coalition Aims to Address Behavioral Targeting" (Apr. 2008), *http://antispywarecoalition.org/newsroom/20080425press.htm.*

[18] 18 U.S.C. § 2511.

Act, ECPA and relevant state wiretap laws to the use of ISP data for behavioral advertising is attached as Appendix B.

As several Members of Congress have noted, the Cable Communications Policy Act also applies here.[19] The law prohibits cable operators from collecting or disclosing personally identifiable information without prior consent[20] While the term "personally identifiable information" in the law is defined by what it does not include—"any record of aggregate data which does not identify particular persons"[21]—we doubt that a user's entire Web traffic stream, unique to that individual, often containing both PII and non-PII, would be considered aggregate data as that term is commonly understood.

We do not believe that it is possible to shoehorn the collection and disclosure of a subscriber's entire browsing history for advertising purposes into the statute's exception for collection or disclosure of information that is necessary to render service.[22] Thus, we conclude that cable-based ISPs that wish to disclose customer information to advertising networks would also have to meet the consent requirements of the Cable Communications Policy Act.

The ISP models that have been deployed thus far have failed to obtain affirmative, express opt-in consent required by law. Several small U.S. ISPs, for example, have failed to meet this threshold requirement, burying vague information about their deals with NebuAd in the ISPs' terms of service.[23] Charter Communications, the largest U.S. ISP that had planned to partner with NebuAd, notified its subscribers that they would be receiving more relevant ads, but did not explain its plans to intercept subscribers' traffic data, and did not provide a way for subscribers to give or withhold consent. Charter has since suspended its plans.

Designing a robust opt-in consent system for ISP-based behavioral advertising presents a formidable challenge. We are less than sanguine that such a system can be easily designed, particularly since it must not only provide a way for consumers to give affirmative consent, but it must also provide a method for them to revoke that consent. The burden is on those who wish to move forward with the model to demonstrate that an express notice and consent regime can work in this context.

VI. The Limits of Self-Regulation

For almost a decade, the primary privacy framework for the behavioral advertising industry has been provided by the Network Advertising Initiative, a self-regulatory group of online advertising networks formed in response to pressure from the Federal Trade Commission and consumer advocates in the wake of privacy concerns over the merger of ad network DoubleClick and Abacus, an offline data broker. NAI members agree to provide consumers with notice and, at minimum, a method to opt out of behavioral advertising. They further pledged to use information collected only for marketing purposes. While at the time of their release CDT welcomed the NAI principles as an important first step, we also noted then that there were flaws in the approach that needed to be addressed and that self-regulation was not a complete solution. The FTC agreed, concluding in its July 2000 report to Congress that "backstop legislation addressing online profiling is still required to fully ensure that consumers' privacy is protected online."[24] That remains true today.

Eight years after the creation of the principles, few consumers are aware of behavioral advertising and fewer still have been able to successfully navigate the confusing and complex opt-out process.[25] Although individual NAI companies have

---

[19] House Representative Edward Markey and House Representative Joe Barton, *Letter to Charter Communications CEO in Regards to the Charter-NebuAd Data Collection Scheme* (May 2008) *http://markey.house.gov/docs/telecomm/ letter_charter_comm_privacy.pdf*. A 1992 amendment adding the phrase "other services" to the Cable Act's privacy provision made it clear that the law covers Internet services provided by cable operators.

[20] 47 U.S.C. § 551(b)–(c).

[21] *Id.* § 551(a)(2)(A).

[22] *Id.* § 551(a)(2)(B).

[23] *See* Mike Masnick, "Where's The Line Between Personalized Advertising And Creeping People Out?," *TechDirt* (Mar. 2008), *http://www.techdirt.com/articles/ 20080311/121305499.shtml;* Peter Whoriskey, "Every Click You Make," *The Washington Post* (Apr. 2008), *http://www.washingtonpost.com/wp-dyn/content/article/2008/04/03/AR2008040304052.html?nav=hcmodule*.

[24] Federal Trade Commission, *Online Profiling: A Report to Congress* (Jul. 2000), *http://www.ftc.gov/os/2000/07/onlineprofiling.htm*.

[25] The drawbacks of opt-out cookies have been well documented: they are confusing for the majority of consumers who do not understand the technology and counter-intuitive to those who are accustomed to deleting their cookies to protect their privacy. Cookies are susceptible to accidental deletion and file corruption. While the NAI is in the process of updating the principles, it has not proposed changes to the opt-out regime. *See* Center for Democracy and Technology, *Applying the FTC's Spyware Principles to Behavioral Advertising: Comments of the Center for*

launched their own consumer awareness initiatives, more work remains to be done.[26] For those consumers who successfully opt out, the NAI's reliance on flawed opt-out cookies means that user preferences are often not persistently honored.

In addition, the NAI's guidelines for the use of sensitive information have never been adequate to guard consumer privacy. Until recently, the definition was limited to a narrowly defined set of PII. While the definition is being revised, it still falls far short of what is needed to address the increasingly sensitive nature of consumer information online.[27]

Finally, the NAI principles only apply to companies that voluntarily join the Initiative. The NAI has no way to force companies to join; the current membership is missing numerous behavioral advertising firms, including some key industry players. In addition, measures to ensure compliance and transparency have withered on the vine.[28] The original NAI principles provided for independent audits and enforcement against noncompliant members, but the audit results were never made public, and reporting on compliance with the principles has been inconsistent.[29]

For all these reasons, while we encourage more robust self-regulatory efforts, we continue to have doubts about the effectiveness of the self-regulatory framework. As online advertising becomes increasingly complex and data collection becomes more pervasive, Congress and the FTC must step in to ensure that consumer interests are fully protected.

VII. The Role of Congress

Congress should take action to address the significant privacy concerns raised by behavioral advertising:

- As a first step, we urge the Committee to hold a series of hearings to examine specific aspects of behavioral advertising. In particular, we believe that further investigation of new models of behavioral advertising using ISP data is warranted, and that the Committee should explore how current laws such as ECPA, the Wiretap Act and the Cable Communications Policy Act apply. Secondary uses of behavioral advertising profiles for purposes other than marketing also deserve additional investigation and scrutiny, as does the use of sensitive information.
- This Committee should set a goal of enacting in the next year general privacy legislation covering both the online and offline worlds. CDT has long argued for simple, flexible baseline consumer privacy legislation that would protect consumers from inappropriate collection and misuse of their personal information while enabling legitimate business use to promote economic and social value. In principle, such legislation would codify the fundamentals of fair information practices, requiring transparency and notice of data collection practices, providing consumers with meaningful choice regarding the use and disclosure of that information, allowing consumers reasonable access to personal information they have provided, providing remedies for misuse or unauthorized access, and setting standards to limit data collection and ensure data security.
- The Federal Trade Commission has played a helpful role in consumer education efforts around behavioral advertising. But it also must exercise its authority under its deception and unfairness jurisdiction to issue enforceable guidelines for behavioral advertising. We ask the Committee to strongly urge the Commis-

---

Democracy and Technology in regards to the FTC Town Hall, "Ehavioral Advertising: Tracking, Targeting, and Technology" (Oct. 2007), *http://www.cdt.org/privacy/20071019CDTcomments.pdf* at 8.

[26] *See, e.g.,* AOL, *Mr. Penguin* (last visited Jul. 2008), *http://corp.aol.com/o/mr-penguin/;* Yahoo!, *Customized Advertising* (last visited Jul. 2008), *http://info.yahoo.com/relevantads/;* Google, *The Google Privacy Channel* (last visited Jul. 2008), *http://youtube.com/user/googleprivacy.*

[27] Center for Democracy and Technology, *Comments Regarding the NAI Principles 2008: The Network Advertising Initiative's Self-Regulatory Code of Conduct for Online Behavioral Advertising* (June 2008), *http://www.cdt.org/privacy/20080612__NAI__comments.pdf* at 6–9.

[28] CDT testing has revealed that only a tiny fraction of companies that collect data that could be used for behavioral advertising are NAI members. *See* Center for Democracy and Technology, *Statement of The Center for Democracy and Technology before The Antitrust, Competition Policy and Consumer Rights Subcommittee of the Senate Committee on the Judiciary on "An Examination of the Google-DoubleClick Merger and the Online Advertising Industry: What Are the Risks for Competition and Privacy?"* (Sept. 2007), *http://www.cdt.org/privacy/20070927committee-statement.pdf.*

[29] *See* Pam Dixon, *The Network Advertising Initiative: Failing at Consumer Protection and at Self-Regulation* (Nov. 2007), *http://www.worldprivacyforum.org/pdf/WPF__NAI__report__Nov2__2007fs.pdf* at 16–17.

sion to exercise the full measure of its enforcement authority over online advertising practices.

- Congress should also examine and strengthen existing communications privacy laws to cover new services, technologies and business models with consistent rules. ECPA was passed more than 20 years ago, long before there was a World Wide Web and the Internet became integrated into Americans' daily lives. The application of the law to common online activities including Web search remains unclear and the legal protections it provides for the enormous amounts of personal data stored online are far too low.
- Finally, Congress should encourage the FTC to investigate how technology can be harnessed to give consumers better control over their online information. The lack of effective controls and the difficulty that consumers have in exercising choice about their participation in online tracking and targeting was the motivation behind the "Do Not Track" list idea proposed by CDT and nine other consumer and privacy groups.[30] Although the proposal has been controversial, the idea behind Do Not Track is both simple and important: provide consumers with an easy-to-use, technology-neutral, persistent way to opt out of behavioral advertising. Congress should promote further study of this idea and other innovative ways to put consumers in control of their information.

VIII. Conclusion

I would like to thank the Committee again for holding this important hearing. We believe that Congress has a critical role to play in ensuring that privacy is protected in an increasingly complex online advertising environment. CDT looks forward to working with the Committee as it pursues these issues further.

APPENDIX A

Simplified Illustration of a Traditional Online Ad Network

Figure 1 below shows a simplified version of a traditional online ad network. Ad networks contract with advertisers on one side and publishers on the other. They take the ads they receive from advertisers and match them to open ad spaces on publisher sites.

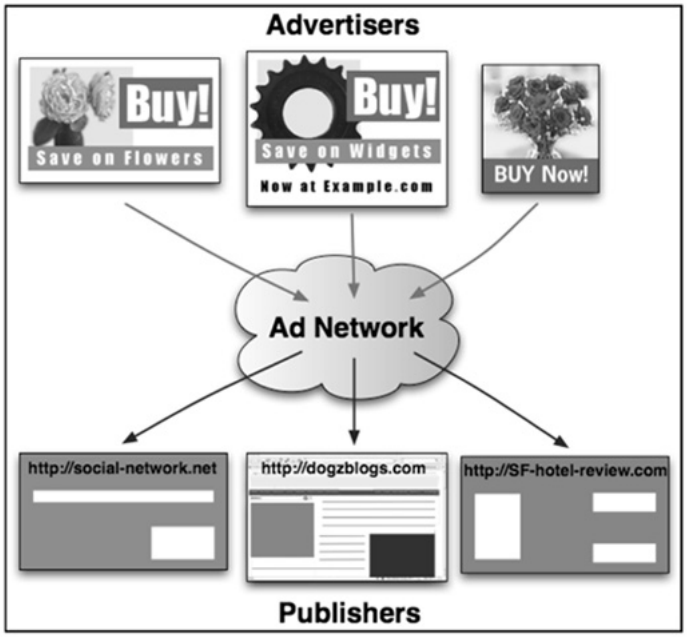

Figure 1.

[30] *See* Pam Dixon et al, *Consumer Rights and Protections in the Behavioral Advertising Sector* (Oct. 2007), *http://www.cdt.org/privacy/20071031consumerprotectionsbehavioral.pdf*.

Figure 2 shows how an ad network collects data about a consumer's web activities. When the consumer first visits a publisher site in the network (*SF-hotel-review.com*), the ad network places a cookie with a unique ID (12345) on the consumer's computer. When the user subsequently visits other publisher sites in the network (including *dogzblogs.com* and *social-network.net*), the cookie containing the ID is automatically transmitted to the ad network. This allows the ad network to keep track of what sites the consumer has visited and build a behavioral profile based on that information, linked to the cookie ID.

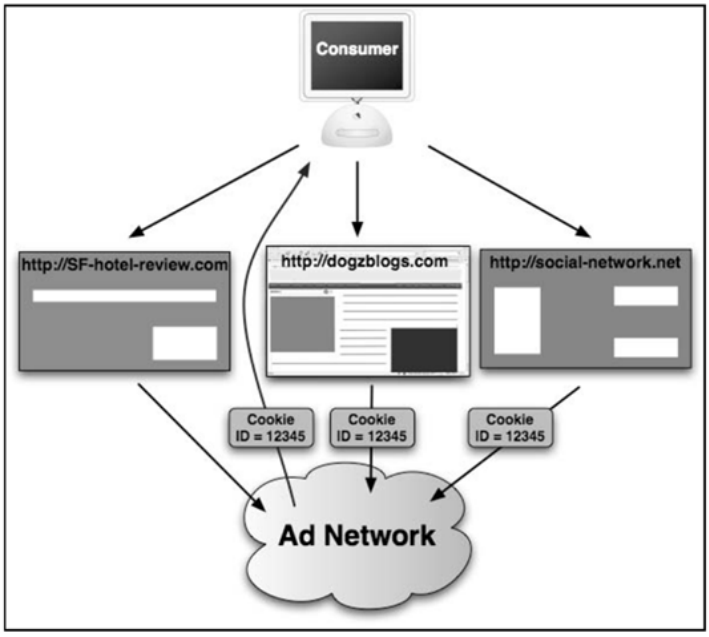

Figure 2.

APPENDIX B

An Overview of the Federal Wiretap Act, Electronic Communications Privacy Act, and State Two-Party Consent Laws of Relevance to the NebuAd System and Other Uses of Internet Traffic Content from ISPs for Behavioral Advertising—July 8, 2008

Much of the content on the Internet (just like content in newspapers, broadcast TV, radio and cable) is supported in whole or part by advertising revenue. The Internet offers special opportunities to target ads based on the expressed or inferred interests of the individual user. There are various models for delivering targeted ads online. These range from the purely contextual (everyone who visits a travel site sees the same airline ad) to models that involve compiling information about the online behavior of individual Internet users, to be used in serving them advertisements. For years, websites have entered into agreements with advertising networks to use "cookies" to track individual users across websites in order to compile profiles. This approach has always been, and remains, a source of privacy concern, in part because the conduct usually occurs unbeknownst to most Internet users. Recent developments, including the mergers between online service providers and some of the largest online advertising networks, have heightened these concerns. The Center for Democracy and Technology has been conducting a major project on behavioral advertising, in which we have been researching behavioral advertising practices, consulting with Internet companies and privacy advocates, developing policy proposals, filing extensive comments at the FTC, and analyzing industry self-regulatory guidelines.

This memo focuses on the implications of a specific approach to behavioral advertising being considered by Internet advertising networks and Internet Service Providers (ISPs). This new approach involves copying and inspecting the content of

each individual's Internet activity with the cooperation of his or her ISP.[31] Under this new model, an advertising network strikes a deal with an ISP, and the ISP allows the network to copy the contents of the individual Web traffic streams of each of the ISP's customers. The advertising network analyzes the content of these traffic streams in order to create a record of each individual's online behaviors and interests. Later, as customers of the ISP surf the Web and visit sites where the advertising network has purchased advertising space, they see ads targeted based on their previous Internet behavior.

NebuAd is one such advertising network company operating in the United States. In the past few months, it has come to light that NebuAd was planning to partner with Charter Communications, a cable broadband ISP, to conduct trials of the NebuAd behavioral advertising technology. Several other smaller ISPs, such as Wide Open West (WOW!), CenturyTel, Embarq, and Knology, have also announced plans with NebuAd to trial or deploy its behavioral advertising technology. In response to concerns raised by subscribers, privacy advocates, and policymakers, Charter, CenturyTel and Embarq have delayed these plans, but NebuAd and other similar companies are continuing to seek new ISP partners.

The use of Internet traffic content from ISPs for behavioral advertising is different from the "cookie"-based model in significant ways and raises unique concerns.[32] Among other differences, it copies all or substantially all Web transactions, including visits to sites that do not use cookies. Thus, it may capture not only commercial activity, but also visits to political, advocacy, or religious sites or other noncommercial sites that do not use cookies.

In this memo, we conclude that the use of Internet traffic content from ISPs may run afoul of Federal wiretap laws unless the activity is conducted with the consent of the subscriber.[33] To be effective, such consent should not be buried in terms of service and should not be inferred from a mailed notice. We recommend prior, express consent, but we do not offer here any detailed recommendations on how to obtain such consent in an ISP context. Also, we note that that the California law requiring consent of all the parties to a communication has been applied by the state Supreme Court to the monitoring of telephone calls when the monitoring is done at a facility outside California. The California law so far has not been applied to Internet communications and it is unclear whether it would apply specifically to the copying of communications as conducted for behavioral monitoring purposes, but if it or another state's all-party consent rule were applied to use of Internet traffic for behavioral profiling, it would seem to pose an insurmountable barrier to the practice.

I. Wiretap Act

A. Service Providers Cannot "Divulge" The Contents of Subscriber Communications, Except Pursuant to Limited Exceptions

The Federal Wiretap Act, as amended by the Electronic Communications Privacy Act, protects the privacy of wire, oral, and electronic communications.[34] "[E]lectronic communication" is defined as "any transfer of signs, signals, writing, images, sounds, data, or intelligence of any nature transmitted in whole or in part by a wire, radio, electromagnetic, photoelectronic or photooptical system . . .."[35] Web browsing and other Internet communications are clearly electronic communications protected by the Wiretap Act.

In language pertinent to the model under consideration, § 2511(3) of the Act states that "a person or entity providing an electronic communication service to the pubic shall not intentionally divulge the contents of any communications . . . while in

---

[31] *See, e.g.,* Peter Whoriskey, *Every Click You Make, Wash. Post* (Apr. 3, 2008), *http://www.washingtonpost.com/wpdyn/content/article/2008/04/03/AR2008040304052.html?nav=hcmodule;* Saul Hansell, *I.S.P. Tracking: The Mother of All Privacy Battles, N.Y. Times: Bits Blog* (Mar. 20, 2008), *http://bits.blogs.nytimes.com/2008/03/20/isp-tracking-the-mother-of-all-privacy-battles/?scp=1-b&sq= the+mother+of+all+privacy+battles&st=nyt*.

[32] Privacy concerns also apply to advertising-based models that have been developed for services, such as e-mail, that ride over ISP networks. *See* CDT Policy Post 10.6, *Google GMail Highlights General Privacy Concerns,* (Apr. 12, 2004), *http://www.cdt.org/publications/policyposts/2004/6* (recommending express prior opt-in for advertising-based e-mail service).

[33] Additional questions have been raised under the Cable Communications Policy Act. *See* Rep. Edward Markey and Rep. Joe Barton, *Letter to Charter Communications CEO in Regards to the Charter-NebuAd Data Collection Scheme* (May 2008), *http://markey.house.gov/docs/telecomm/letter_charter_comm_privacy.pdf*. In this memo, we focus on issues arising under the Federal Wiretap Act, as amended by the Electronic Communications Privacy Act.

[34] 18 U.S.C. §§ 2510–2522.

[35] *Id.* § 2510(12).

transmission on that service to any person or entity other than an addressee or intended recipient. . . .”[36]

There are exceptions to this prohibition on disclosure, two of which may be relevant here. One exception specifies that “[i]t shall not be unlawful under this chapter for an . . . electronic communication service, whose facilities are used in the transmission of a[n] . . . electronic communication, to intercept, disclose, or use that communication in the normal course of his employment while engaged in any activity which is a *necessary incident to the rendition of his service* or to the protection of the rights or property of the provider of that service.”[37] We will refer to this as the “necessary incident” exception. The second exception is for disclosures with the consent of one of the parties.[38] We will discuss both exceptions below. We conclude that only the consent exception applies to the disclosure of subscriber content for behavioral advertising, and we will discuss preliminarily what “consent” would mean in this context.

B. With Limited Exceptions, Interception Is Also Prohibited

The Wiretap Act regulates the “interception” of electronic communications. The Act defines “intercept” as the “acquisition of the contents of any . . . electronic . . . communication through the use of any electronic, mechanical, or other device.”[39]

The Wiretap Act broadly bars all intentional interception of electronic communications.[40] The Act enumerates specific exceptions to this prohibition.[41] Law enforcement officers, for example, are authorized to conduct interceptions pursuant to a court order. For ISPs and other service providers, there are three exceptions that might be relevant. Two we have mentioned already: the “necessary incident” exception and a consent exception.[42]

A third exception, applicable to interception but not to disclosure, arises from the definition of “intercept,” which is defined as acquisition by an “electronic, mechanical, or other device,” which in turn is defined as “any device or apparatus which can be used to intercept a[n] . . . electronic communication *other than*—(a) any telephone or telegraph instrument, equipment or facility, or any component thereof . . . (ii) being used by a provider of . . . electronic communication service in the *ordinary course of its business*. . . .”[43] This provision thus serves to limit the definition of “intercept,” providing what is sometimes called the “telephone extension” exception, but which we will call the “business use” exception.

C. The Copying of Internet Content for Disclosure to Advertising Networks Constitutes Interception

When an ISP copies a customer’s communications or allows them to be copied by an advertising network, those communications have undoubtedly been “intercept[ed].”[44] Therefore, unless an exception applies, it seems likely that placing a device on an ISP’s network and using it to copy communications for use in developing advertising profiles would constitute illegal interception under § 2511(1)(a); similarly, the disclosure or use of the intercepted communications would run afoul of § 2511(1)(c) or § 2511(1)(d), respectively.

---

[36] *Id.* § 2511(3)(a). Lest there be any argument that the disclosure does not occur while the communications are “in transmission,” we note that the Stored Communications Act (SCA) states that “a person or entity providing an electronic communication service to the public shall not knowingly divulge to any person or entity the contents of a communication while in electronic storage by that service.” *Id.* § 2702(a)(1). We do not comment further here on the SCA because, in our judgment, the approach that has been described so far clearly involves the divulging of communications “while in transmission.”

[37] *Id.* § 2511(2)(a)(i) (emphasis added). This analysis focuses on the capture of electronic communications and definitions are abridged accordingly.

[38] *Id.* § 2511(3)(b)(ii).

[39] *Id.* § 2510(4).

[40] *Id.* § 2511(1).

[41] *Id.* § 2511(2).

[42] Separate from the consent provision for disclosure, the consent exception for interception is set forth in 18 U.S.C. § 2511(2)(d): “It shall not be unlawful under this chapter for a person not acting under color of law to intercept a[n] . . . electronic communication where such person is a party to the communication or where one of the parties to the communication has given prior consent to such interception. . . .”

[43] *Id.* § 2510(5) (emphasis added).

[44] *See, e.g., United States* v. *Rodriguez,* 968 F.2d 130, 136 (2d Cir. 1992) (holding in context of telephone communications that “when the contents of a wire communication are captured or redirected in any way, an interception occurs at that time” and that “[r]edirection presupposes interception”); *In re State Police Litig.,* 888 F. Supp. 1235, 1267 (D. Conn. 1995) (stating in context of telephone communications that “it is the act of diverting, and not the act of listening, that constitutes an ‘interception’”).

D. The "Necessary Incident" Exception Probably Does Not Permit the Interception or Disclosure of Communications for Behavioral Advertising Purposes

The Wiretap Act permits interception of electronic communications when the activity takes place as "a necessary incident to the rendition of [the ISP's] service or to the protection of the rights or property of the provider of that service."[45] The latter prong covers anti-spam and anti-virus monitoring and filtering and various anti-fraud activities, but cannot be extended to advertising activities, which, while they may enhance the service provider's revenue, do not "protect" its rights. Courts have construed the "necessary incident" prong quite strictly, requiring a service provider to show that it *must* engage in the activity in order to carry out its business.[46] It is unlikely that the copying, diversion, or disclosure of Internet traffic content for behavioral advertising would be construed as a "necessary incident" to an ISP's business. Conceivably, an ISP could argue that its business included copying its subscribers communications and providing them to third parties for purposes of placing advertisements on websites unaffiliated with the ISP, but the ISP would probably have to state that that business existed and get the express agreement of its customers that they were subscribing to that business as well as the basic business of Internet access, which leads anyhow to the consent model that we conclude is necessary.

E. While It Is Unclear Whether the "Business Use" Exception Would Apply to the Use of a Device Installed or Controlled by a Party Other than the Service Provider, the Exception Does Not Apply to the Prohibition Against Divulging a Subscriber's Communications

The "business use" exception, § 2510(5)(a), constricts the definition of "device" and thereby narrows the definition of "intercept" in the Wiretap Act. There are two questions involved in assessing applicability of this exception to the use of Internet traffic content for behavioral advertising: (1) whether the device that copies the content for delivery to the advertising network constitutes a "telephone or telegraph instrument, equipment or facility, or any component thereof," and (2) whether an ISP's use of the device would be within the "ordinary course of its business."

We will discuss the "business use" exception at some length, because there has been considerable discussion already about whether copying of an ISP subscriber's communications for behavioral advertising is an "interception" under § 2511(1) of the Wiretap Act. However, even if the business use exception applied, an ISP would only avoid liability for the *interception* of electronic communications. It would still be prohibited from divulging the communications of its customers to an advertising network under the separate section of the Wiretap Act, § 2511(3), which states that a service provider "shall not intentionally divulge the contents of any communication . . . while in transmission on that service to any person or entity other than an addressee or intended recipient. . . ."[47] The business use exception does not apply to this prohibition against divulging.[48]

At first glance, it would seem that the business use exception is inapplicable to the facilities of an ISP because the exception applies only to a "telephone or telegraph instrument, equipment or facility, or any component thereof." However, the courts have recognized that ECPA was motivated in part by the "dramatic changes in new computer and telecommunications technologies"[49] and therefore was intended to make the Wiretap Act largely neutral with respect to its treatment of various communications technologies. The Second Circuit, for example, concluded in a related context that the term "telephone" should broadly include the "instruments,

---

[45] 18 U.S.C. § 2511(2)(a)(i).

[46] *See United States* v. *Councilman,* 418 F.3d 67, 82 (1st Cir. 2005) (en banc) (holding that service provider's capture of e-mails to gain commercial advantage "clearly" was not within service provider exception); *Berry* v. *Funk,* 146 F.3d 1003, 1010 (D.C. Cir. 1998) (holding in context of telephone communications that switchboard operators' overhearing of a few moments of phone call to ensure call went through is a "necessary incident," but anything more is outside service provider exception).

[47] 18 U.S.C. § 2511(3)(a).

[48] By adopting two different exceptions—"necessary incident" and "ordinary course"—Congress apparently meant them to have different meanings. Based on our reading of the cases, the necessary incident exception is narrower than the ordinary course exception. It is significant that the "necessary incident" exception applies to both interception and disclosure while the "ordinary course" exception is applicable only to interception. This suggests that Congress meant to allow service providers broader latitude in examining (that is, "intercepting" or "using") subscriber communications so long as they did not disclose the communications to third parties. This permits providers to conduct a range of in-house maintenance and service quality functions that do not involve disclosing communications to third parties.

[49] S. Rep. No. 99–541, at 1 (1986), *reprinted in* 1986 U.S.C.C.A.N. 3555.

equipment and facilities that ISPs use to transmit e-mail."[50] Therefore, as a general matter, it should be assumed that the business use exception is available to ISPs.

However, it is not certain that the device used to copy and divert content for behavioral advertising would be considered to be a component of the service provider's equipment or facilities. In some of the behavioral advertising implementations that have been described, the monitoring device or process is not developed or controlled by the ISP but rather by the advertising network.

The second question is whether an ISP's use of a device to copy traffic content for behavioral advertising falls within the "ordinary course of its business." There are a number of cases interpreting this exception, but none of them clearly addresses a situation where a service provider is copying all of the communications of its customers. Many of the cases arise in situations where employers are monitoring the calls of their employees for purposes of supervision and quality assurance. "These cases have narrowly construed the phrase 'ordinary course of business.'"[51] Often such cases also involve notice to the employees and implied consent.[52] One court has stated that, even if an entity could satisfy the business use exception, notice to one of the parties being monitored would be required.[53] Other cases involve the monitoring of prisoners.

Some cases have interpreted "ordinary course" to mean anything that is used in "normal" operations. The D.C. Circuit, for instance, has suggested that monitoring "undertaken normally" qualifies as being within the "ordinary course of business."[54] In the context of law enforcement taping of the phone calls of prisoners, the Ninth and Tenth Circuits have concluded that something is in the "ordinary course" if it is done routinely and consistently.[55] It might be that courts would give equal or greater latitude to service providers in monitoring their networks than they would give to mere subscribers or users.

Other circuit courts have used a more limited interpretation, concluding that "ordinary course" only applies if the device is being used to intercept communications for "legitimate business reasons."[56] Although the courts have not been entirely clear as to what that means, some have suggested that it is much closer to necessity than to mere profit motive.[57] One frequently-cited case explicitly holds that the business use exception does not broadly encompass a company's financial or other motivations: "The phrase 'in the ordinary course of business' cannot be expanded to mean anything that interests a company."[58]

Normal principles of statutory interpretation would require that some independent weight be given to the word "ordinary," so that the exception does not encompass anything done for business purposes. It is unclear, however, how much weight courts would give to the word "ordinary" in a rapidly changing market. It does not seem that the phrase "ordinary course of business" should preclude innovation, but courts might refer to past practices and normal expectations surrounding a line of business and specifically might look to what customers have come to expect.

Viewed one way, it is hard to see how the copying of content for behavioral advertising is part of the "ordinary course of business" of an ISP. After all, the ISP is not the one that will be using the content to develop profiles of its customers; the profiling is done by the advertising network, which does not even disclose to the ISP the profiles of its own subscribers. (The profiles are proprietary to the advertising

---

[50] *Hall* v. *Earthlink Network, Inc.,* 396 F.3d 500, 505 (2d Cir. 2005) (quoting S. Rep. No. 99–541 at 8).

[51] *United States* v. *Murdock,* 63 F.3d 1391. 1396 (6th Cir 1995).

[52] *E.g., James* v. *Newspaper Agency Corp.,* 591 F.2d 579 (10th Cir. 1979).

[53] *See, e.g., Adams* v. *City of Battle Creek,* 250 F.3d 980, 984 (6th Cir. 2001).

[54] *Berry* v. *Funk,* 146 F.3d 1003, 1009 (D.C. Cir. 1998) (workplace monitoring).

[55] *See United States* v. *Van Poyck,* 77 F.3d 285, 292 (9th Cir. 1996); *United States* v. *Gangi,* 57 Fed. Appx. 809, 814 (10th Cir. 2003).

[56] *See Arias* v. *Mutual Central Alarm Serv., Inc.,* 202 F.3d 553, 560 (2d Cir. 2000) (monitoring calls to an central alarm monitoring service).

[57] *See id.* (concluding that alarm company had legitimate reasons to tap all calls because such businesses "are the repositories of extremely sensitive security information, including information that could facilitate access to their customers' premises"); *see also First* v. *Stark County Board of Comm'rs,* 234 F.3d 1268, at *4 (6th Cir. 2000) (table disposition).

[58] *Watkins* v. *L.M. Berry & Co.,* 704 F.2d 577, 582 (11th Cir. 1983). Watkins states: "We hold that a personal call may not be intercepted in the ordinary course of business under the exemption in section 2510(5)(a)(i), except to the extent necessary to guard against unauthorized use of the telephone or to determine whether a call is personal or not. In other words, a personal call may be intercepted in the ordinary course of business to determine its nature but never its contents." 704 F.2d at 583. This language supports the conclusion that the business use exception could not cover wholesale interception of ISP traffic, no more than switchboard operators can perform wholesale monitoring of telephone traffic.

network and it is careful not to disclose them to anyone.) Very few (if any) of the ads that are placed using the profiles will be ads for the ISP's services; they will be ads for products and services completely unrelated to the ISP's "ordinary course of business." Moreover, the ads will be placed on websites having no affiliation with the ISP. On the other hand, the ISP could argue that part of its business model—part of what keeps its rates low—is deriving revenue from its partnership with advertising networks.

The legislative histories of the Wiretap Act and ECPA weigh against a broad reading of the business use exception. Through these laws, Congress intended to create a statutory regime generally affording strong protection to electronic communications. Congress included limited, specific and detailed exceptions for law enforcement access to communications, and other limited, specific and detailed exceptions to allow companies providing electronic communications service to conduct ordinary system maintenance and operational activities. Congress gave especially high protection to communications content. If the business use exception can apply any time an ISP identifies a new revenue stream that can be tapped though use of its customers' communications, this careful statutory scheme would be seriously undermined.

F. The Consent Exception: The Context Weighs Heavily in Favor of Affirmative, Opt-In Consent from ISP Subscribers

Consent is an explicit exception both to the prohibition against intercepting electronic communications under the Wiretap Act and to the Act's prohibition against disclosing subscriber communications. The key question is: How should consent be obtained for use of Internet traffic content for behavioral advertising? Courts have held in telephone monitoring cases under the Wiretap Act that consent can be implied, but there are relatively few cases specifically addressing consent and electronic communications. However, in cases involving telephone monitoring, one circuit court has stated that consent under the Wiretap Act "is not to be cavalierly implied."[59] Another circuit court has noted that consent "should not casually be inferred"[60] and that consent must be "actual," not "constructive."[61] Yet another circuit court has stated: "Without actual notice, consent can only be implied when the surrounding circumstances *convincingly* show that the party knew about and consented to the interception."[62] Furthermore, "knowledge of the *capability* of monitoring alone cannot be considered implied consent."[63] The cases where consent has been implied involve very explicit notice; many of them involve the monitoring of prisoners' phone calls.[64]

Consent is context-based. It is one thing to imply consent in the context of a prison or a workplace, where notice may be presented as part of the daily log-in process. It is quite another to imply it in the context of ordinary Internet usage by residential subscribers, who, by definition, are using the service for personal and often highly sensitive communications. Continued use of a service after a mailed notice might not be enough to constitute consent. Certainly, mailing notification to the bill payer is probably insufficient to put all members of the household who share the Internet connection on notice.

Thus, it seems that an assertion of implied consent, whether or not users are provided an opportunity to opt out of the system, would most likely not satisfy the consent exception for the type of interception or disclosure under consideration here. Express prior consent (opt-in consent) is clearly preferable and may be required. While meaningful opt-in consent would be sufficient, courts would likely be skeptical of an opt-in consisting merely of a click-through agreement—*i.e.,* a set of terms that a user agrees to by clicking an on-screen button—if it displays characteristics typical of such agreements, such as a large amount of text displayed in a small box,

---

[59] *Watkins.* 704 F.2d at 581 ("Consent under title III is not to be cavalierly implied. Title III expresses a strong purpose to protect individual privacy by strictly limiting the occasions on which interception may lawfully take place.").

[60] *Griggs-Ryan* v. *Smith,* 904 F.2d 112, 117 (1st Cir. 1990).

[61] *In re Pharmatrak, Inc. Privacy Litig.,* 329 F.3d 9, 20 (1st Cir. 2003); *see also United States* v. *Corona-Chavez,* 328 F.3d 974, 978 (8th Cir. 2003).

[62] *Berry* v. *Funk,* 146 F.3d 1003, 1011 (D.C. Cir. 1998) (internal quotation omitted).

[63] *Watkins,* 704 F.2d at 581; *see also Deal* v. *Spears,* 980 F.2d 1153, 1157 (8th Cir. 1992) (holding that consent not implied when individual is aware only that monitoring might occur, rather than knowing monitoring is occurring).

[64] "The circumstances relevant to an implication of consent will vary from case to case, but the compendium will ordinarily include language or acts which tend to prove (or disprove) that a party knows of, or assents to, encroachments on the routine expectation that conversations are private. And the ultimate determination must proceed in light of the prophylactic purpose of Title III—a purpose which suggests that consent should not casually be inferred." *Griggs-Ryan,* 904 F.2d at 117.

no requirement that the user scroll through the entire agreement, or the opt-in provision buried among other terms of service.[65]

In regards to consent, the model under discussion here is distinguishable from the use of "cookies," which were found to be permissible by a Federal district court in a 2001 case involving DoubleClick.[66] In that case, the websites participating in the DoubleClick advertising network were found to be parties to the communications of the Internet users who visited those sites. As parties to the communications, the websites could consent to the use of the cookies to collect information about those communications. Here, of course, the ISPs are not parties to the communications being monitored and the interception or disclosure encompasses communications with sites that are not members of the advertising network. Therefore, the source of consent must be the IPS's individual subscribers, as it would be impossible to obtain consent from every single website that every subscriber may conceivably visit.

II. State Laws Requiring Two-Party Consent to Interception

A. Summary

In addition to the Federal Wiretap Act, a majority of states have their own wiretap laws, which can be more stringent than the Federal law. Most significantly, twelve states[67] require all parties to consent to the interception or recording of certain types of communications when such interception is done by a private party not under the color of law.

In several of these states—for example, Connecticut—the all-party consent requirement applies only to the recording of oral conversations. In others, the all-party consent rule extends to both voice and data communications. For example, Florida's Security of Communications Act makes it a felony for any individual to intercept, disclose, or use any wire, oral, or electronic communication, unless that person has obtained the prior consent of all parties[68] Similarly, the Illinois statute on criminal eavesdropping prohibits a person from "intercept[ing], retain[ing], or transcrib[ing an] electronic communication unless he does so . . . with the consent of all of the parties to such . . . electronic communication."[69]

The most important all-party consent law may be California's, because the California Supreme Court held in 2006 that the law can be applied to activity occurring outside the state.

B. California

The 1967 California Invasion of Privacy Act makes criminally liable any individual who "intentionally taps, or makes any unauthorized connection . . . or who willfully and without the consent of all parties to the communication . . . reads, or attempts to read, or to learn the contents or meaning of any message . . . or communication while the same is in transit or passing over any wire, line, or cable, or is being sent from, or received at any place" in California.[70] It also establishes liability for any individual "who uses, or attempts to use, in any manner . . . any information so obtained" or who aids any person in doing the same.[71] The law has a separate section creating liability for any person eavesdropping upon or recording a confidential communication "intentionally and without the consent of all parties," whether the parties are present in the same location or communicating over telegraph, telephone, or other device (except a radio).[72]

Consent can be implied only in very limited circumstances. The California State Court of Appeals held in *People* v. *Garber* that a subscriber to a telephone system is deemed to have consented to the telephone company's monitoring of his calls if he uses the system in a manner that reasonably justifies the company's belief that he is violating his subscription rights, and even then the company may only monitor

---

[65] *See, e.g., Specht* v. *Netscape Commc'ns Corp.,* 306 F.3d 17 (2d Cir. 2002) (rejecting online arbitration agreement because, among other things, site permitted customer to download product without having scrolled down to arbitration clause and agreement button said only "Download"); *United States* v. *Lanoue,* 71 F.3d 966, 981 (1st Cir. 1995) ("Deficient notice will almost always defeat a claim of implied consent.").

[66] *In re DoubleClick Inc. Privacy Litig.,* 154 F.Supp.2d 497 (S.D.N.Y. 2001).

[67] The twelve states are California, Connecticut, Florida, Illinois, Maryland, Massachusetts, Michigan, Montana, Nevada, New Hampshire, Pennsylvania, and Washington.

[68] Fla. Stat. § 934.03(1).

[69] Ill. Comp Stat. 5/14–1(a)(1).

[70] Cal. Pen. Code § 631(a).

[71] *Id.*

[72] *Id.* § 632(a). The statute explicitly excludes radio communications from the category of confidential communications.

his calls to the extent necessary for the investigation.[73] An individual can maintain an objectively reasonable expectation of privacy by explicitly withholding consent for a tape recording, even if the other party has indicated an intention to record the communication.[74]

In *Kearney* v. *Salomon Smith Barney, Inc.,* the state Supreme Court addressed the conflict between the California all-party consent standard and Georgia's wiretap law, which is modeled after the Federal one-party standard.[75] It held that, where a Georgia firm recorded calls made from its Georgia office to residents in California, the California law applied. The court said that it would be unfair to impose damages on the Georgia firm, but prospectively the case effectively required out-of-state firms having telephone communications with people in California to announce to all parties at the outset their intent to record a communication. Clear notice and implied consent are sufficient. "If, after being so advised, another party does not wish to participate in the conversation, he or she simply may decline to continue the communication."[76]

C. The Implications of Kearney

The *Kearney* case arose in the context of telephone monitoring, and there is a remarkable lack of case law addressing whether the California statute applies to Internet communications. If it does, or if there is one other state that applies its all-party consent rule to conduct affecting Internet communications across state lines, then no practical form of opt-in, no matter how robust, would save the practice of copying Internet content for behavioral advertising. That is, even if the ISP only copies the communications of those subscribers that consent, and the monitoring occurs only inside a one-party consent state, as soon as one of those customers has a communication with a non-consenting person (or website) in an all-party consent state that applies its rule to interceptions occurring outside the state, the ISP would seem to be in jeopardy. The ISP could not conceivably obtain consent from every person and website in the all-party consent state. Nor could it identify (for the purpose of obtaining consent) which people or websites its opted-in subscribers would want to communicate with in advance of those communications occurring.

A countervailing argument could be made that an all-party consent rule is not applicable to the behavioral advertising model, since the process only copies or divulges one half of the communication, namely the half from the consenting subscriber.

III. Conclusion

The practice that has been described to us, whereby an ISP may enter into an agreement with an advertising network to copy and analyze the traffic content of the ISP's customers, poses serious questions under the Federal Wiretap Act. It seems that the disclosure of a subscriber's communications is prohibited without consent. In addition, especially where the copying is achieved by a device owned or controlled by the advertising network, the copying of the contents of subscriber communications seems to be, in the absence of consent, a prohibited interception. Affirmative express consent, and a cessation of copying upon withdrawal of consent, would probably save such practices under Federal law, but there may be state laws requiring all-party consent that would be more difficult to satisfy.

Senator DORGAN. Ms. Harris, thank you very much. We appreciate your testimony.

Mr. Chris Kelly is the Chief Privacy Officer for Facebook Incorporated. Mr. Kelly, you may proceed.

STATEMENT OF CHRIS KELLY, CHIEF PRIVACY OFFICER, FACEBOOK, INC.

Mr. KELLY. Thank you very much, Chairman Dorgan and Members of the Committee, for the opportunity to address the Committee about the important privacy matters facing the online advertising industry.

---

[73] 275 Cal. App. 2d 119 (Cal. App. 1st Dist. 1969).
[74] *Nissan Motor Co.* v. *Nissan Computer Corp.,* 180 F. Supp. 2d 1089 (C.D. Cal. 2002).
[75] 39 Cal. 4th 95 (2006).
[76] *Id.* At 118.

I am Chris Kelly, the Chief Privacy Officer of Facebook, a social service on the Internet that serves more than 80 million active users, about 30 million of whom are in the United States.

Facebook aims to create social value by empowering people to share their lives and experiences with the people they care about. From the founding of the company in a dorm room in 2004 until today, Facebook's privacy settings have given users control over who has access to their personal information by allowing them to choose the friends they accept and the networks they join.

We are dedicated to developing advertising that is relevant and personal and to transparency with our users about how we use their information in the advertising context. We are pleased to discuss both Facebook's general approach to privacy and how these principles have been implemented in advertising provided by Facebook.

With many mainstream media reports focusing on privacy concerns about social networking sites, we first want to clarify how our site differs from most. Though we will not always address user concerns perfectly—no site can—Facebook is committed to empowering users to make their own choices about what information they share and with whom they share it.

The statement that opens our privacy policy, a short, plain English introduction, is the best place to start this discussion. It reads: "We built Facebook to make it easy to share information with your friends and people around you. We understand you may not want everyone in the world to have the information you share on Facebook; that is why we give you control of your information. Our default privacy settings limit the information displayed in your profile to your networks and other reasonable community limitations we tell you about."

Facebook follows two core principles:

First, you should have control over your personal information. Facebook helps you share information with your friends and people around you. You choose what information you put in your profile, including contact and personal information, pictures, interests and groups that you join. And you control the users with whom you share that information through the privacy settings on the Privacy page.

Two, you should have access to the information that others want to share. There is an increasing amount of information available out there, and you may want to know what relates to you, your friends, and people around you. We want to help you easily get that information.

Sharing information should be easy. And we want to provide you with the privacy tools necessary to control how and with whom you share that information. If you have any questions or ideas, please send them to *privacy@facebook.com,* the e-mail address that we regularly monitor.

We implement these principles through our friend and network architectures and through controls that are built into every one of our innovative products. Contrary to common public reports, full profile data on Facebook is not even available to most users on Facebook, let alone all users of the Internet. Users have extensive and precise controls available to choose who sees what among their

networks and friends, as well as tools that give them the choice to make a limited set of information available to search engines and other outside entities.

The privacy link that appears in the upper right-hand corner of every Facebook page allows users to make these choices whenever they are using the site, and everyday use of the site educates users as to the meaning of privacy controls. For instance, a user will see regularly that they have access to the profiles of their friends and those who share a network with them, but not to profiles of those who are neither friends nor network members.

In February 2008, Facebook simplified and streamlined its presentation of privacy settings to users, adopting a common lock icon throughout the site to denote the presence of a user-configurable privacy setting. We also introduced the concept of "Friends Lists" which, when paired with privacy settings, allow users to easily configure subsets of their confirmed friends who may see certain content. We are constantly looking for means to give users more effective control over their information and to improve communications with users and the general public about our privacy architecture so that they can make their own choices about what they want to reveal.

I want to say a few words about privacy and advertising on Facebook. It is important to stress in the first instance that targeting of advertising generally benefits users. But we have revealed in our privacy policy for nearly 3 years the following. We have had the following statement present. "Facebook may use information in your profile without identifying you as an individual to third parties. We do this for purposes such as aggregating how many people in a network like a band or a movie and personalizing advertisements and promotions so that we can provide you Facebook. We believe this benefits you. You can know more about the world around you and, where there are advertisements, they are more likely to be interesting to you. For example, if you put a favorite movie in your profile, we might serve you an advertisement highlighting a screening of a similar one in your town. But we don't tell the movie company who you are."

This critical distinction that we embrace in our policies and practices and that we want users to understand is between the use of personal information for advertisements in personally identifiable form and the use, dissemination, or sharing of information with advertisers in non-personally identifiable form. Ad targeting that shares or sells personally identifiable information to advertisers without user control is fundamentally different from targeting that only gives advertisers the ability to present their ads based on aggregate data.

And with that, I see that my time is up. So I look forward to answering your questions. Thank you.

[The prepared statement of Mr. Kelly follows:]

PREPARED STATEMENT OF CHRIS KELLY, CHIEF PRIVACY OFFICER, FACEBOOK, INC.

Thank you, Mr. Chairman, for the opportunity to address the Committee about the important privacy matters facing the online advertising industry.

I am Chris Kelly, the Chief Privacy Officer of Facebook, a social service on the Internet that serves more than 80 million active users, roughly 30 million of whom are in the United States.

Facebook aims to create social value by empowering people to share their lives and experiences with the people they care about. From the founding of the company in a dorm room in 2004 to today, Facebook's privacy settings have given users control over who has access to their personal information by allowing them to choose the friends they accept and networks they join.

We are dedicated to developing advertising that is relevant and personal, and to transparency with our users about how we use their information in the advertising context. We are pleased to discuss both Facebook's general approach to privacy and how these principles have been implemented in advertising provided by Facebook.

With many mainstream media reports focusing on privacy concerns about "social networking sites," we first want to clarify how our site differs from most. Though we will not always address user concerns perfectly—no site can—Facebook is committed to empowering users to make their own choices about what information they share, and with whom they share it.

I. Facebook and Privacy

The statement that opens our privacy policy, a short plain-English introduction, is the best place to start this discussion. It reads:

> We built Facebook to make it easy to share information with your friends and people around you. We understand you may not want everyone in the world to have the information you share on Facebook; that is why we give you control of your information. Our default privacy settings limit the information displayed in your profile to your networks and other reasonable community limitations that we tell you about.

Facebook follows two core principles:

> 1. You should have control over your personal information.
> Facebook helps you share information with your friends and people around you. You choose what information you put in your profile, including contact and personal information, pictures, interests and groups you join. And you control the users with whom you share that information through the privacy settings on the Privacy page.
>
> 2. You should have access to the information others want to share.
> There is an increasing amount of information available out there, and you may want to know what relates to you, your friends, and people around you. We want to help you easily get that information.
>
> Sharing information should be easy. And we want to provide you with the privacy tools necessary to control how and with whom you share that information. If you have questions or ideas, please send them to *privacy@facebook.com*.

We implement these principles through our friend and network architectures, and through controls that are built into every one of our innovative products. Contrary to common public reports, full profile data on Facebook isn't even available to most users on Facebook, let alone all users of the Internet. Users have extensive and precise controls available to choose who sees what among their networks and friends, as well as tools that give them the choice to make a limited set of information available to search engines and other outside entities.

The "privacy" link that appears in the upper-right hand corner of every Facebook page allows users to make these choices whenever they are using the site, and everyday use of the site educates users as to the meanings of privacy controls. For instance, a user will see regularly that they have access to the profiles of their friends and those who share a network, but not to the profiles of those who are neither friends nor network members.

In February 2008, Facebook simplified and streamlined its presentation of privacy settings to users, adopting a common lock icon throughout the site to denote the presence of a user-configurable privacy setting. We also introduced the concept of "Friends Lists," which, when paired with privacy settings, allow users to easily configure a subset of their confirmed friends who may see certain content. We are constantly looking for means to give users more effective control over their information and to improve communications with users and the general public about our privacy architecture so they can make their own choices about what they want to reveal.

For instance, we participated in the Federal Trade Commission's workshop on new advertising technologies, and have been working with government officials and nongovernmental organizations throughout the globe. Facebook has also worked productively with state and Federal officials, as well as law enforcement, to explain our longstanding strategy to make the Internet safer by promoting responsibility and identity online, and is currently participating in the state Attorneys General Internet Safety Technical Task Force.

II. Privacy and Advertising on Facebook

A. Personally Identifiable and Non-Personally Identifiable Information

It is important to stress here in the first instance that targeting of advertising generally benefits users. Receiving information that is likely to be relevant, whether paid for by an advertiser or not, leads to a better online experience. Facebook aims to be transparent with our users about the fact that advertising is an important source of our revenue and to explain to them fully the uses of their personal data they are authorizing by using Facebook. For instance, the following explanation of how we use information for advertising has been a prominent part of our privacy policy for nearly 3 years:

> Facebook may use information in your profile without identifying you as an individual to third parties. We do this for purposes such as aggregating how many people in a network like a band or movie and personalizing advertisements and promotions so that we can provide you Facebook. We believe this benefits you. You can know more about the world around you and, where there are advertisements, they're more likely to be interesting to you. For example, if you put a favorite movie in your profile, we might serve you an advertisement highlighting a screening of a similar one in your town. But we don't tell the movie company who you are.

The critical distinction that we embrace in our policies and practices, and that we want users to understand, is between the use of personal information for advertisements in personally-identifiable form, and the use, dissemination, or sharing of information with advertisers in non-personally-identifiable form. Ad targeting that shares or sells personal information to advertisers (name, e-mail, other contact oriented information) without user control is fundamentally different from targeting that only gives advertisers the ability to present their ads based on aggregate data. Most Facebook data is collected transparently in personally identifiable form—users know they are providing the data about themselves and are not forced to provide particular information.[1] Sharing information on the site is limited by user-established friend relationships and user-selected networks that determine who has access to that personal information. Users can see how their data is used given the reactions of their friends when they update their profiles, upload new photos or videos, or update their current status.

On Facebook, then, a feedback loop is established where people know what they are uploading and receive timely reactions from their friends, reinforcing the fact they have uploaded identifiable information. The privacy policy and the users' experiences inform them of how advertising on the service works—advertising that enables us to provide the service for free to users is targeted to the expressed attributes of a profile and presented in the space on the page allocated for advertising, without granting an advertiser access to any individual user's profile.

Furthermore, advertising on Facebook is subject to guidelines designed to avoid deceptive practices, and with special restrictions and review with respect to any advertising targeted at minors.

I cannot stress strongly enough that Facebook does not authorize access by the Internet population at large, including advertisers, to the personally identifiable information that a user willingly uploads to Facebook. Facebook profiles have extensive user-configurable rules limiting access to information contained in them. Unless a user decides otherwise by willingly sharing information with an advertiser—for instance, through a contest—advertisers may only target advertisements against non-personally identifiable attributes about a user of Facebook derived from profile data.

We recognize that other Internet services may take a different approach to advertisers and the information available to them. Advertising products that sell personally identifiable information to advertisers without user permission, that rely on transforming non-personally identifiable information into personally identifiable information without robust notice and choice to users, or that rely on data collection that a user has scant notice of and no control over, raise fundamentally different privacy concerns. Facebook does not offer such products today and has no intention of doing so. Advertising products founded on the principles of transparency and user control, where data is collected directly from users in personally identifiable space

---

[1] Currently, only four pieces of data are required to establish and maintain a Facebook account—e-mail address to provide a unique login identifier, birthdate to calculate age, name to provide a standard identifier (our Terms of Use require real name), and gender to promote the accuracy of grammar through the site infrastructure.

and targeting is done based on aggregate or characteristic data in non-personally identifiable space, respect the principle that sits at the heart of privacy concerns.

B. History of Facebook Ads and Beacon

Perhaps because our site has developed so quickly, we have sometimes been inartful in communicating with our users and the general public about our advertising products. It therefore may be fruitful to provide a brief history of the current Facebook advertising offerings, including Facebook Ads and Social Ads, as well as the Beacon product that garnered significant public attention late last year.

In November 2007, Facebook introduced Facebook Ads, which consisted of both a basic self-service targeting infrastructure based on the non-personally identifiable use of keywords derived from profile data, and Social Ads, which allow for the paid promotion of certain interactions users take online to those users' friends in conjunction with an advertiser message. The basic targeting infrastructure of Facebook Ads is quite similar to many other Internet advertising systems, where media buyers and agencies can purchase guarantees that their advertisements will run to people who have certain characteristics, often expressed (as they are in Facebook Ads) in "keywords," or in demographic categories such as men between 29 and 34.

Social Ads are an innovation in that they allow advertisers to pay for promotion of certain interactions users take online to those users' friends. For example, if I become a supporter of a particular political figure on Facebook, their campaign could pay to promote that fact to more of my friends than would have been informed of it otherwise through the Facebook News Feed, and potentially pair a message from the campaign with it. It is notable first that only my action can trigger a Social Ad and that Social Ads are only presented to confirmed friends as opposed to the world at large; there will be no Social Ad generated noting my action to anyone but a confirmed friend. It is also notable that in this paid promotion context through Social Ads, an advertiser is not purchasing and does not have access to users' personal data—they are only told that a certain number of users have taken relevant actions and the number of ads generated by those actions.

We introduced at the same time as Facebook Ads a product called Beacon to allow users to bring actions they take on third-party sites into Facebook. Our introduction of this product with advertising technology led many to believe that Beacon was an ad product when it really was not. Participating third party sites do not pay Facebook to offer Beacon, nor must a third party site that wants to use Beacon purchase Facebook Ads. No Facebook user data is sold to or shared with these third party sites. In most cases, Beacon pertains to non-commercial actions like the playing of a game or the adding of a recipe to an online recipe box. In other cases, we and the participating third party sites experimented with capturing purchases for sharing within a user's Facebook friend network, obviously a more commercial enterprise. In both the non-commercial and commercial contexts, we discovered in the weeks after launch that users felt they did not have adequate control over the information and how it was being shared with their friends.

We quickly reached the conclusion that Beacon had inadequate built-in controls driving user complaints, helped along by an organized campaign by *MoveOn.org* to get us to alter the product. We made significant changes within weeks after its launch to make it a fully opt-in system. We remain convinced that the goal of helping users share information about their activities on the web with their friends is desirable and appreciated. Indeed, a number of services now exist which attempt to help users in this way. While Beacon was cast in the mainstream press as an advertising product, it operates fundamentally as a means to connect, with a user's permission and control, actions elsewhere on the web with a user's Facebook friend network.

We are currently working on the next generation of Facebook's interactions with third party websites, called Facebook Connect, to empower users further to share content and actions with their friends using the Facebook infrastructure, and are focused on assuring that proper controls are built into this system.

III. FTC Principles on Behavioral Targeting

Finally, we would like to reinforce our earlier positive public comments about the Federal Trade Commission's leadership in addressing privacy concerns about how data is collected and shared online.

As explained above, Facebook Ads are materially different from behavioral targeting as it is usually discussed, but given our goals of transparency and user control, the important corollary of ensuring appropriate security and the goal of providing users notice and choice with respect to service changes, we applaud the FTC's desire to establish principles in the online advertising area. We believe the FTC should expand and enhance the discussion in the principles about the distinction be-

tween personally and non-personally identifiable information to clarify the need for different treatment of advertising based on those different types of information. We will continue our participation in discussion of the principles as they evolve.

Thank you again, Mr. Chairman, for the opportunity to share our views, and I am happy to answer any questions you may have.

ATTACHMENT

Microsoft's Leadership on Consumer Privacy—July 2008

Microsoft has a long-standing commitment to consumer privacy and we have put that commitment into action. Here are some examples:

Broad Self-regulatory Approach for Online Advertising. Microsoft recently filed comments with the Federal Trade Commission explaining the need for a broad self-regulatory privacy approach to online advertising, noting that all online advertising activities involve data collection from users and therefore have privacy implications.

Meaningful Online Advertising Principles. In July 2007, Microsoft announced five fundamental privacy principles for online search and ad targeting. These principles include commitments to user notice, user control, search data anonymization, security, and best practices.

Clear and Upfront User Notice. Microsoft was one of the first companies to develop so-called "layered" privacy notices that give clear and concise bullet-point summaries of our practices and direct users to a place where they can find more information. We post a link to this user-friendly privacy notice on every one of our web pages.

Robust User Control. Microsoft has recently deployed a robust method to enable users to opt out of behavioral advertising. Specifically, users can now tie their opt-out choice to their Windows Live ID so their choice can work across multiple computers and be more persistent (for example, deleting cookies will not erase their opt-out selection). We also highlight the availability of this opt-out choice on the first layer of our privacy notice.

Unique Steps To De-Identify Data. Microsoft is unique in our use of a technical method (known as a one-way cryptographic hash) to separate search terms from account holders' personal information, such as name, e-mail address, and phone number, and to keep them separated in a way that prevents them from being easily recombined. We have also relied on this method to ensure that we use only data that does not personally identify individual consumers to serve ads online.

Strict Search Data Anonymization. Microsoft will anonymize all search data after 18 months, which we believe is an appropriate time-frame in our circumstances to enable us to maintain and improve the security, integrity and quality of our services. In addition, unlike other companies, we will irreversibly remove the *entire* IP address and other cross-session identifiers, such as cookies and other machine identifiers, from search terms after 18 months.

Support for Federal and State Privacy Legislation. Microsoft has actively supported state legislation that would impose baseline notice, choice, and security requirements on entities that collect data to serve online ads. We also were one of the first companies to advocate for comprehensive Federal privacy legislation in the United States.

Dedicated Privacy Personnel and Processes. Microsoft was one of the first companies to appoint a chief privacy officer, an action we took nearly a decade ago, and we currently employ over 40 employees who focus on privacy full-time, and another 400 who focus on it as part of their jobs. We have made significant investments in privacy in terms of dedicated personnel and training and by building robust privacy standards into our product development and other business processes.

Guidelines for Third Parties. Microsoft is committed to helping others in industry protect consumers' privacy interests. For example, we have released a set of privacy guidelines designed to help developers build meaningful privacy protections into their software programs and online services.

Consumer Education and Private-Public Sector Partnerships. Microsoft has taken steps to educate consumers about ways to protect themselves while online, and we have worked closely with industry members and law enforcement around the world to identify security threats, share best practices, and improve our coordinated response to privacy, security and other Internet safety issues.

Senator DORGAN. Mr. Kelly, thank you very much. We appreciate your testimony.

We will now hear from Mr. Clyde Wayne Crews, Jr., Vice President for Policy, Director of Technology Studies at the Competitive Enterprise Institute. Mr. Crews, welcome.

STATEMENT OF CLYDE WAYNE CREWS, JR., VICE PRESIDENT FOR POLICY/DIRECTOR OF TECHNOLOGY STUDIES, COMPETITIVE ENTERPRISE INSTITUTE

Mr. CREWS. Thank you very much. Good morning, Mr. Chairman. I appreciate the opportunity to appear.

Online behavioral marketing is not the devil, but with emergent technologies like biometrics on the horizon, data privacy debates like the ones we are facing today are only going to intensify. Targeted advertising helps fuel today's flood of information, frictionless e-commerce, and the global blogger soapbox. It has become cliché to note that the Internet is one of the most important wealth-creating and democratizing technologies ever known.

But behavioral marketing stokes privacy fears. Is my data personally identifiable? Can it become so? Will my identity be stolen, and if a breach occurs, who is punished?

Note that we were all angry when ads were untargeted spam. Now that ads are relevant, well, we are still not satisfied.

Behavioral advertising employs heretofore unexploited capabilities of the Internet, reinforcing the reality that there is much more to the Internet than the web at any one juncture. It is only 2008.

User preferences preclude one-size-fits-all privacy policy. Online some hide behind digital gated communities. Others parade in front of personal webcams. Privacy is not a thing to legislate. It is a relationship expressed in countless ways. Legislation would be complex. If online privacy is regulated, what about offline? Should the standard be opt-in or opt-out? Who defines behavioral or sensitive? Should state laws be preempted? What about noncommercial information collection?

Industry already follows principles like the FTC's proposed opt-out for sensitive information even when the information is not personally identifiable, but the rise of the information society amid a homeland security culture is an unfortunate coincidence. Blurring of public and private databases complicates things. Programs like Total Information Awareness, CAPPSII, and a national ID undermine privacy when data cannot be confined to an agreed-upon business purpose.

Government often does not need to protect privacy but to allow it in the first place. One is reminded of the old *Peanuts* cartoon of Snoopy sitting on top of the doghouse typing "Dear IRS, please remove my name from your mailing list."

Another old joke goes that if McDonald's were giving away free Big Macs in exchange for a DNA sample, there would be lines around the block.

But consumers do care. The Net itself enables collective consumer discontent, such as blog backlashes we have seen against companies. The result: firms alter their information handling procedures without law. Consumers can also avoid certain sites or use Anonymizer or Scroogle or TrackMeNot or a virtual private network. Choice mandates are not persuasive when choice is increasingly the default.

This debate's fury implies that real market opportunities exist in providing online anonymity. A marketer does not necessarily want to know who you are but how somebody like you acts. No one in a free market is really lucky enough to self-regulate as FTC puts it. Firms are regulated by consumer fury, rivals, by Wall Street, by intolerant investors. There is no such thing as no regulation. The choice we face is between political discipline or competitive discipline in an impatient market. Even companies on the frontier of behavioral advertising like Phorm and NebuAd face discipline. One's sympathies there are going to depend upon the ownership status one accords to a web page. But today's web page is not what tomorrow's web page is going to be with information and ads coming into the page from numerous sources.

Privacy standards best thrive as a war between computer scientists. Marketing to an unidentified customer is today's happy goal, but at the very same time, there is great value in technologies that prevent others from posing as us. That is one reason the use of personally identifiable data should not be ruled out altogether.

Meanwhile, we need improved cyberinsurance products and enhanced liability products to evolve online. Regulating can short-circuit such market innovations. The private sector needs practice for the really difficult cases like the emergence of biometrics.

Privacy policies are already legally binding. Thus, a more fitting Federal agenda would target identity theft and computer crime and enforce privacy policies and stay neutral on computer science, keep compulsory databases separate from private ones, stabilize Government's own insecure networks, and avoid interventions like data retention that undermine security guarantees.

To protect consumers online, we must consciously avoid entrenching regulations such that effective private alternatives and institutions, however warranted, simply cannot emerge. Online marketers are today's battered business bureau, but they need battering by competitive discipline, not just legislation.

Thank you very much.

[The prepared statement of Mr. Crews follows:]

PREPARED STATEMENT OF CLYDE WAYNE CREWS, JR., VICE PRESIDENT FOR POLICY/DIRECTOR OF TECHNOLOGY STUDIES, COMPETITIVE ENTERPRISE INSTITUTE

The Competitive Enterprise Institute (CEI) is a non-profit public policy research foundation dedicated to individual liberty, limited government, and markets. We appreciate the opportunity to discuss policy issues surrounding online advertising.

Privacy dilemmas are inevitable on the frontiers of an evolving information era, but CEI maintains that competitive approaches to online privacy and security will be more nimble and effective than rigid political mandates at safeguarding and enhancing consumer well-being, facilitating commerce and wealth creation, and even contributing to the rise of the anonymous approaches to commerce we'd like to see.

The Rise of Privacy and Cybersecurity as Public Policy Issues

The marvelous thing about the Internet is that one can contact and learn about anyone and anything. The downside is that the reverse is often true. The digital information age—against a backdrop of rising globalization—offers consumers unprecedented access to news, information, democratized credit and much more. Anyone may collect and share information on any subject, corporation, government—or in many cases, other individuals.

Companies from retailers to search engines to software makers all collect consumer data—enough to fill vast server warehouses. Of course, websites have long collected and marketed information about visitors. The latest twist is that behavioral marketing firms "watch" our clickstreams to develop profiles or inform cat-

egories to better target future advertisements. Unarguably beneficial, the process stokes privacy concerns. Fears abound over the data's security; is any of it personally identifiable? If not, can it conceivably become so? Will personal information fall into the wrong hands? Will it become public? And if a breach occurs, who's punished? While Capitol Hill, beltway regulators or state governments are seen often as the first line of defense, regulatory and legislative proposals, much like the anti-spam law, can fall short of success. Aspirations can exceed actual legislative capability.

Clearly, as a technological phenomenon, mass transactional data tracking and collection are here to stay; and with nascent technologies like biometrics that could fully authenticate users on the horizon, the debates will only intensify.

Along with behavioral advertising, new data-mining and biometrics technologies promise higher levels of convenience and, ultimately, more secure commerce online. Beyond the "merely" commercial, the technologies also hint at greater physical security in the "homeland" and in our workplaces via authentication.

On the upside, online advertising enables today's familiar subscription-fee-free cornucopia of news and information, and the free soapbox enjoyed by bloggers worldwide. It's become cliché to note the commercialized Internet is one of the most important wealth-creating sectors and democratizing technologies ever known. Benefits to society range from frictionless e-commerce, to the democratization of privileges once available only to the rich, to a megaphone for all.

This online bounty has also brought real and imagined privacy vulnerabilities to the forefront, ranging from personal identity theft to exposure of private thoughts and behavior online. Once, we could contend merely with nuisances like spam, cookie-collection practices and the occasional spyware eruption. Since policies today are being formulated in the context of a post-Sept. 11 world, cybersecurity and computerized infrastructure access and security join routine privacy as prime policy issues. Adding complexity is the noted emergence of biometric technologies and highly engineered data mining that could alter the future of behavioral marketing. Thus we must contend not just with run of the mill commercial aspects of privacy policies, but with national security themes and what some consider a dangerous new surveillance state.

The question is, do newfangled data collection techniques threaten fundamental expectations of privacy, and in the case of government data collection, even liberty itself?

What principles distinguish between proper and improper uses of personal information, and what policies maximize beneficial e-commerce and consumer welfare? Business use of behavioral advertising can be irritating, but many have made peace with advertisers' using personal information. One-size-fits-all privacy mandates will undermine e-commerce and the consumer benefits we take for granted. Sweeping regulations can especially harm start-ups that lack the vast data repositories already amassed by their larger competitors. Our policies should be consistent with tomorrow's entrepreneurs (and consumers) starting businesses of their own to compete with the giants of today.

Thus, privacy policies need to be filtered through the lens of the entire society's needs. We must consider the impact on: (1) consumers, (2) e-commerce and commerce generally, (3) broader security, cybersecurity, homeland security and critical infrastructure issues, and finally (4) citizen's 4th amendment protections.

Happily the prospect of billions in economic losses from mistakes incentivize the market's efforts to please consumers and safeguard information and networks.

Web Functionality Continues to Unfold

The recent emergence of behavioral advertising reinforces the easily forgotten reality that there's more to the Internet than the "Web" at any given juncture; it's only 2008, and there are doubtless more commercially valuable avenues for marketing yet to be discovered in the decades ahead. Targeted, behavioral and contextual advertising make use of heretofore unexploited underlying capabilities of the Internet, possibilities that hadn't yet occurred to anyone else, just as the original banner ad trailblazers first did years ago—and, yes, just as the spammers did.

At the Outset: Policy Must Distinguish Between Public and Private Data

Parameters are needed to talk coherently about the treatment of individual's data. Information acquired through the commercial process must be kept separate from that extracted through government mandates. Similarly, private companies generally should not have access to information that government has forced individuals to relinquish (what one might call the "Social Security" problem). Private industry should generate its own marketing-related information (whether "personally identifiable" or not), for purposes limited by consumer acceptance or rejection, rather than

piggyback on government IDs. Confidentiality is a value, and should be a competitive feature.

Conversely, for any debate over behavioral advertising to make sense, corporate America needs to be able to make credible privacy assurances to the public. People need to know that the data they relinquish is *confined to an agreed-upon business, transactional or record-keeping purpose,* not incorporated in a government database. If regulators end up routinely requiring banks, airlines, hotels, search engines, software companies, Internet service providers and other businesses to hand over private information (in potentially vulnerable formats), *they will not only undermine evolving commercial privacy standards, including behavioral, but make them impossible.* Government's own information security practices is the elephant in the room when it comes to contemplating e-commerce sector's stance with respect to privacy. It's all too easy to give the online marketing industries a black eye and risk turning society against the technologies, and ensure regulation and politicization. Private data and public data policies are potentially on a collision course, but need not be.

The benefits that personalization brings, like easier, faster shopping experiences, are in their infancy. Sensible data collection improves search, communication, ability to innovate, U.S. competitiveness—all the things we associate with a well-functioning economy and evolution in healthy consumer convenience and power.

Privacy Legislation: Premature and Overly Complex

In contemplating government's role with respect to privacy and information security, we must recognize the realities of differing user preferences that preclude one-size-fits-all privacy and security policy. Online, there are exhibitionists and hermits. Some hide behind the equivalent of gated communities; others parade less-than-fully clothed before personal webcams.

Note how we work ourselves up into a lather: policymakers were concerned about privacy when ads were *untargeted and irrelevant* (spam); now a solution—behavioral and contextual marketing—makes ads relevant, and we're hand-wringing about privacy there too. Incidentally, spam was framed as a privacy problem, but in reality the spammer didn't typically know who you were. Likewise, a positive early development in behavioral advertising is that personally identifiable information is not always crucial to the marketer (although sensible uses of personally identifiable information should not be thwarted). Too often, the complaint seems to be *commerce as such.* For example, the Federal Communications Commission recently decided to investigate the "problem" with embedded ads in TV programming.[1]

Policy should recognize privacy is not a single "thing" for government to protect; it is a *relationship* expressed in countless ways. That relationship is best facilitated by emergent standards and contracts—like the Network Advertising Initiative's behavioral advertising principles[2] that predate the Federal Trade Commission's late 2007 principles[3]—and in emergent market institutions like identity theft insurance. Apart from varied privacy preferences, any legislative effort to regulate behavioral advertising gets exceedingly complex:

- If online privacy is regulated, what about offline?
- Should behavioral advertising be opt-in or opt-out? (Why and when?)
- Who defines which advertising is "behavioral"?
- What is the legislative line between sensitive, and non-sensitive, personally identifiable information?
- Should the Federal Government pre-empt state privacy laws?
- Will the privacy rules apply to government?
- Will government abstain from accessing or seizing private databases?
- What about *non-commercial* information collection? (Will the rules apply to bloggers? Or to Facebook activism?)
- What about consumer harm caused by privacy legislation (Given that in the business world, most transactions occur between strangers.)
- What of practical problems of written privacy notices? (Especially given the declining importance of the desktop, the emergent web-like multi-sourced nature of web-pages themselves, smaller wireless-device screens, and the "thing-to-thing" Net that bypasses humans altogether.)

---

[1] Associated Press, "FCC to look into embedded advertising on TV," *MSNBC.com*. June 26, 2008. *http://www.msnbc.msn.com/id/25401193/*.

[2] *http://www.networkadvertising.org/networks/principles_comments.asp.*

[3] Federal Trade Commission, "Behavioral Advertising, Moving the Discussion Forward to Possible Self-Regulatory Principles," December 20, 2007. *http://www.ftc.gov/os/2007/12/P859900stmt.pdf.*

- Could disclosure and reporting mandates create a burdensome paperwork requirements detrimental to small businesses? (A privacy "Sarbanes-Oxley")
- What about the right to remain anonymous; Behavioral marketing appears to be on course to facilitate anonymous transactions; will government permit it? How should tolerance of anonymity differ in commercial and political contexts?

The Internet was designed as an open, non-secure network of semi-trusted users. Thus one interpretation of the nature of the cyberspace is that advertisers may legitimately assemble information on what is clearly a very public network that never offered any real pretense of security. But even assuming one's online pursuits can be tracked, privacy tools nonetheless are emerging, and vendors must be held to commitments. Given legislation's complications and the Internet's inherent security limitations, a rational policy prescription should be more limited: *Hold the private sector accountable to the contracts and guarantees it makes, and target identity theft and the criminals who perpetrate it.* If legislation merely does such things as send bad actors overseas, we merely create regulatory hassles for mainstream companies that already follow "best practices," and for small businesses trying to make a go of legitimate e-commerce.

As in spam debate, we face less a legislative problem than a technological one. It's true that social norms and expectations have yet to gel—but those are as varied as individuals are.

***Marketing* Is Not Today's Dominant Information Collection Threat**

The emphasis on online privacy legislation could represent a case of misdirected energy. The most important information collection issues of the day are not related to mere *marketing;* rather, criminals who ignore already existing laws and will ignore any new law, are the ones creating mischief online, abusing the trust we have or would like to have in vendors. Meanwhile, *government* surveillance and information collection threaten liberties and *genuine* privacy—and one cannot "opt out." (One is reminded of the *Peanuts* cartoon of Snoopy sitting on his doghouse typing, "Dear IRS . . . Please remove my name from your mailing list.")[4]

The stringent opt-in standard some seek in the behavioral marketing debate is not one government tolerates for itself. The post-Sept. 11 push for compulsory national ID cards, warrant-less wiretapping and escalating data retention mandates signify a government more inclined toward infringing privacy than acting as guarantor.

The rise of the information society amid a "homeland security culture" is an unfortunate coincidence, an accident, but one that colors debates over marketing that would otherwise be more pedestrian. The tendency of government to interfere with privacy practices is undeniable: Total Information Awareness, CAPPSII, and a national ID are examples of expansive government efforts that would undermine the private sector's freedom and ability to make privacy assurances in the first place.

Worse, when technology companies contract with government for information services, they would very likely request immunity for data breaches by extension of the Homeland Security Act that grants similar immunities for failed security technologies; so if markets are tempted to repudiate self-regulation and liability for privacy standards, government oversight becomes the default. The "homeland security culture" can undermine the market's entrepreneurial tendency to resolve the dilemmas created by information sharing.

Deliberations over privacy and online security should start with the recognition that government often doesn't need to protect our privacy, it needs to *allow it in the first place.* Business, whatever missteps happen in behavioral marketing, can deliver. As it stands, nobody's in any position to make ironclad security guarantees given the open nature of the Internet, but the Web is a giant research experiment, and techniques will improve. In fact, as behavioral tracking does begin to employ personally identifiable information, security benefits in ways that people will approve. The Net's governmental origins have left privacy expectations and rights somewhat ill-defined in many online contexts. But we all at times need to identify ourselves and validate the identity of others.

Consumers are Not Powerless: The Redundancy of FTC Standards

In spite the Net's vulnerabilities, consider how legislation pales compared to unforgiving competitive discipline. An old joke holds that if McDonald's was giving away free Big Macs in exchange for a DNA sample, there would be lines around the block. But consumers do care; and thanks to the Internet itself, they are hardly a voiceless mass.

---

[4] *http://www.freerepublic.com/focus/f-news/1384722/posts.*

Every few weeks brings new headlines about government data-handling debacles, such as governmental bodies forcing employees to carry Social Security cards on their person, or the IRS requirement that payment checks feature the SSN.[5] Confidence isn't inspired when the government's information practices lag the private sector's.

Contrast that with what happens to a careless private firm. Google and its recent mergers and alliances put it under scrutiny, but why? (Recall it was Google that in 2006 refused to hand over user search data to the Justice Department; and Google's YouTube division is now being forced by a New York district court to hand over user viewing records in a video piracy case. Google not unsurprisingly objects.) But imagine if Google suffered a serious data breach. Consumers would lose trust, and Google could lose millions. Examples abound of consumer sovereignty, such as the backlash against Facebook's Beacon that cross-posted users shopping activities on friends' sites,[6] and Comcast's de-prioritizing of certain file sharing transfers. Today's Internet users are empowered to educate the world about business practices of which they disapprove. The blogosphere transforms Web users into citizen-journalists, harnessing the power of collective discontent. The result: *Companies routinely change and improve their information handling procedures without law.*

Policies proposed in the name of what consumers want or should want are all too common, as if the ideas hadn't occurred to anyone in the competitive marketplace already, or as if the markets hadn't been forced to adapt already, or as if issues weren't more complicated than the regulators suppose.

For example, the November 2007 FTC proposal on behavioral advertising offers pedestrian principles that have long been in play:[7] Paraphrasing, sites should declare that info is being collected and used and users can opt out; data should be "reasonably secured," and retained only as long as necessary; affirmative consent be given for privacy policy changes; and sensitive information should not be collected at all, or only with affirmative opt-in.

Where do the real incentives lie? Industry looks at what consumers actually want; industry often already embraces opt-in for sensitive information categories, even when the information is not personally identifiable. And if not so empowered by a benevolent vendor, users can already exercise the choice allegedly sought in privacy legislation; they can simply choose not to disclose sensitive information on certain sites, or employ privacy software that can thwart unwanted data collection and allow anonymous Web browsing. "Anonymizer" is still out there for encrypted, anonymous surfing. People can switch to "Scroogle" to disguise their Google searches; A consumer can use a dedicated tool to nullify his identity prior to a sensitive search like "HIV"; TrackMeNot can send out "white noise" search queries to disguise the real one. No mandates for choice are needed; choice is the default, whether vendors prefer it or not.

In terms of competitive enterprise, the divisiveness of a debate like behavioral marketing implies that *real market opportunities exist in providing online anonymity.* After all, despite all the hand-wringing over personally identifiable information, any given marketer doesn't necessarily need to know who *you are,* but how somebody *like you* acts. (Much like a politician seeking a vote, incidentally.) Again, the worry is less that the market is invading our privacy and more whether that anonymity will be permitted politically when it finally is available to us commercially.

"Self-Regulation" Is a Misnomer

Privacy and security need to be competitive features. We need to foster competition in reputations. And we need flexibility when the inevitable mistakes are made.

Businesses compete; and one area in which they can compete is in the development of technologies that enhance security. Washington's inclination toward regulating online consumer relationships threatens to undermine the market's catering to diverse individual privacy preferences, and hinder the evolution of competitive research and innovation in secure applications. Privacy encompasses innumerable relationships between consumers and businesses, and no single set of privacy safeguards is appropriate. While government demands information disclosure, profit-driven firms compete to offer robust privacy assurances. As businesses respond to evolving consumer preferences, stronger privacy policies will emerge.

---

[5] Associated Press, "U.S. Contradicts Itself Over Its Own ID Protection Advice," *SiliconValley.com,* July 2, 2008. *http://www.siliconvalley.com/news/ci_9762027?nclick_check=1.*

[6] Caroline McCarthy, "*MoveOn.org* takes on Facebook's 'Beacon' ads," *CNet News.com.* November 20, 2007. *http://news.cnet.com/8301-13577_3-9821170-36.html.*

[7] Federal Trade Commission, 2007.

Businesses are disciplined by responses of their competitors. Political regulation is pre-mature; but "self-regulation" like that described in the FTC principles is a misnomer; it is *competitive discipline* that market processes impose on vendors. Nobody in a free market is so fortunate as to be able to "self regulate." Apart from the consumer rejection just noted, firms are regulated by the competitive threats posed by rivals, by Wall Street and intolerant investors, indeed by computer science itself.

Neither the government nor private sector has a spotless "self-regulatory" record, but FTC seems unconcerned about the former. Data breaches at businesses, governments and universities rose 69 percent in 2008.[8] Government can contribute to data security by ensuring that its own policies—like data sharing or data retention mandates, or sweeping subpoenas—do not interfere with competitive discipline.

Even governmental calls for self-regulation seem lukewarm. Along with the Federal Trade Commission's Principles on what personally identifiable information firms may collect, a bill in the New York state legislature would impose drastic opt-in standards, preventing companies from gathering personalized information without explicit user permission. When Microsoft bid for Yahoo! this year, the Justice Department almost immediately wondered whether the combined firm would possess "too much" consumer data. Canada recently announced an investigation into Facebook's privacy protections. Now the Department of Justice is investigating the Google-Yahoo deal.[9]

Everybody's heard of Google and Microsoft, but fewer have heard of companies like Phorm and NebuAd, which present the more pertinent behavioral marketing issues; their new techniques give ISPs a dog in the fight, since online advertising is a commercial opportunity impossible for ISPs to ignore. ISPs see Google and Microsoft and they want a piece of the online advertising action too. These companies' techniques have been called spyware, but again, they incorporate the Net's underlying capabilities in novel ways, and they too are subject to competitive discipline. One's sympathies will depend upon the "ownership" status one accords to Web pages, and what one regards as online "trespass." The only certainty is a Web page today is not what a Web page tomorrow will be. Was there ever a real reason for publishers and advertisers to think they could control everything a user saw, given the open-ended potential of software's obvious ability to route content to browsers in novel ways? At many sites, like Facebook, each page is a "Web" in its own right, containing widgets drawing information and ads from numerous sources. The debate has really only just begun, and online marketing trade groups are truly the "Battered Business Bureau." But they're battered by competitive discipline, not merely regulators.

Lessons from Personally Identifiable Data Use Can Inform Future Online Security Practices

A frontier industry requires the flexibility to learn from mistakes. We must distinguish between proper and improper uses of surveillance by *both* the private and public sectors. Not many want to be tracked by the authorities, or treated like human bar code. Myriad benefits will accrue from the further deployment of identification techniques—even personally identifiable—into various facets of daily life. But where is the line crossed, and who is capable of crossing it?

In private hands, techniques like behavioral marketing, biometric and data-mining technologies enlarge our horizons. They expand the possibilities of a market economy by bolstering security in private transactions ranging from face-to-face authentication to long-distance commerce. The best, most secure technologies are those that *prevent others from posing as us*—that's why the value of personally identifiable data cannot be ruled out. The Web is desperately short of that kind of clarity and authentication, in a world of cyber-risks, identity theft, and the need to conduct ever more sensitive transactions. But nothing is automatic. The marketplace imperative requires private sector experimentation in privacy: It's messy, but necessary.

On the one hand, policy should not create situations where companies are required to ask for personal info that otherwise wouldn't be needed. (Google declares in its comments on the FTC advertising principles that obeying certain rules would require it to collect information it otherwise would not need.) On the other hand,

---

[8] Brian Krebs, "Data Breaches Are Up 69% This Year, Nonprofit Says," *Washington Post*. July 1, 2008. p. D3. *http://www.washingtonpost.com/wp-dyn/content/article/2008/06/30/AR2008063002123.html*.

[9] Peter Whoriskey, "Google Ad Deal Is Under Scrutiny," *Washington Post,* July 2, 2008. Page D1. *http://www.washingtonpost.com/wp-dyn/content/article/2008/07/01/AR2008070102622.html.*

certain forms of identifiable behavioral tracking may prove important in specific contexts and shouldn't be prohibited.

Disallowing personally identifiable information is the wrong thing to do. We often need to identify those we're dealing with on line, and for them to be able to identify us; such instruments will be governed by heretofore unknown contracts and privacy polices. It's not "self-regulation," but the needs of the world at large driving this evolution. Rather than legislating, it's likely better to keep this a war between computer scientists; between those working on behavioral advertising with personal information and/or authentication, and those working on behavioral without authentication. Being able to sell to a customer but not have that customer identified is a key research area in computer science. The consumer-control ethos—the notion that we don't have to be tracked—puts consumers, not advertisers, in the drivers' seat Let the computer scientists duke it out.

In many transactions and contexts, the Web needs better authentication, not the abandonment of personally identifiable information. The private sector should experiment with generating such data in ways that consumers can accept. Some say we must regulate because online risks exist; this report argues for *not* regulating because there are online risks. The firms that reduce risks in ways palatable to consumers offer a great service. New products and institutions still need to emerge around online commerce.

Expanding the Marketplace for Liability and Private Security Insurance

Privacy is one subset of the much broader issues of online security and cybersecurity. It's been noted that a basic problem today is that no one stands in any position to make guarantees to anybody about anything. That doesn't mean improved insurance products and enhanced liability contracts won't develop online, however. Lessons learned from spam, privacy, and preventing piracy of intellectual property will carry over to the security issues of tomorrow.

Government shouldn't grant immunity to software companies for breaches, but at the same time it should not impose liability on them either. It's not so clear whom to sue on an Internet not amenable to authentication, but standards will emerge. Government interference can impede private cyber-insurance innovations.

Certain innovations can be sacrificed by regulating. The private sector needs to "practice" now for the really difficult cases like the integration of biometrics into the online world; meanwhile the Federal Government needs to focus on cyber-crime.

A Positive Agenda for the Federal Government

Policymakers should appreciate the government's inherent limitations as well as the vulnerabilities that can be created by Federal policies and procedures.

From lost laptops to hacks into the Pentagon e-mail system, to "D" grades for the Department of Homeland Security's own information security practices, regulators' ability to rationally guide others on privacy is questionable. In many areas it makes sense to circumscribe regulators' sphere of influence, while increasing that of the market.

Recognizing that governments can fail just as markets can, there are numerous ways government within its limitations can *properly* foster private sector innovation in security:

- Foster competitive discipline.
- Emphasize protecting government's own insecure networks, not regulating markets. This means many things, including: removing sensitive information from government websites; limit the size and scope of government databases to ensure government doesn't create artificial cybersecurity risks; avoiding data retention mandates and other interventions that undermine private-sector security guarantees.
- Focus on computer criminals, not cyber-regulations.
- Assess areas where it's best to *liberalize* private sector data-sharing rules. For example, facilitating private sector medical data sharing could deliver benefits to suffering patients. More broadly, some firms cannot share data among their own divisions because of antitrust and privacy strictures. Enhancing cross-firm coordination can improve reliability and security.
- Recognize that commercial anonymity and political anonymity differ; we may need "less" of the former, even as we expand the latter. Research should continue on the seemingly opposed agendas of authentication of users on the one hand, and anonymizing technologies on the other.

Conclusion: Affirming Private Sector Primacy Over Information Practices

Our greatest privacy concern should be government collection of our information, not the emergence of targeted marketing.

In the changing world of e-commerce, the role of government is not to predetermine commercial privacy arrangements, but to enforce information-sharing contracts that companies make between themselves or with individuals. Privacy policies are legally binding. Government's role is not to dictate the structure of privacy contracts through such means as opt-in or opt-out policies; it is to halt deceptive practices and hold private firms accountable to the guarantees they make. Government's other role is to protect citizens from identity theft, which is not a commercial enterprise, but a criminal one.

If anonymity and the inability to exclude bad actors are at the root of genuine online security problems, legislation doesn't make them go away. When contemplating centralized government vs. decentralized market approaches to protection consumers online, we must strive, before regulating, to follow the "cybersecurity commandment": *Don't entrench regulation to such a degree that effective private alternatives and institutions, however warranted as conditions change, simply cannot emerge.*

Related Reading

Wayne Crews and Ryan Radia, "Rigid Federal Mandates Hinder Privacy Technologies," *San Jose Mercury News,* June 15, 2008, *http://www.mercurynews.com/opinion/ci_9593341.*

Wayne Crews, "Cybersecurity Finger-pointing: Regulation vs. Markets for Software Liability, Information Security, and Insurance," *CEI Issue Analysis* 2005 No. 7, May 31, 2005, *http://cei.org/pdf/4569.pdf.*

Wayne Crews, "Cybersecurity and Authentication: The Marketplace Role in Rethinking Anonymity—Before Regulators Intervene," *CEI Issue Analysis* 2004 No. 2, November 8, 2004, *http://cei.org/pdf/4281.pdf.*

Wayne Crews, Comments to the FTC on e-mail authentication themes, September 30, 2004, *http://www.cei.org/pdf/4229.pdf.*

Alberto Mingardi and Wayne Crews, EU takes a Swipe at Google, *International Herald Tribune,* March 9, 2007, *http://www.iht.com/articles/2007/03/09/opinion/edmingardi.php.*

Wayne Crews and Brooke Oberwetter, "Preventing Identity Theft and Data Security Breaches: The Problem With Regulation," *CEI Issue Analysis* 2006 No. 2, May 9, 2006, *http://cei.org/pdf/5316.pdf.*

Wayne Crews "Giving Chase in Cyberspace: Does Vigilantism Against Hackers and File-sharers Make Sense?" *CEI OnPoint* No. 109, October 2, 2006. *http://cei.org/pdf/5569.pdf.*

Wayne Crews, "Trespass in Cyberspace: Whose Ether Is It Anyway?" *TechKnowledge* #19, Cato Institute, September 10, 2001, *http://www.cato.org/tech/tk/010910-tk.html.*

Wayne Crews, "Human Bar Code: Monitoring Biometrics Technologies In a Free Society," Cato Institute Policy Analysis No. 452, September 17, 2002, *http://www.cato.org/pubs/pas/pa452.pdf.*

Senator DORGAN. Mr. Crews, thank you very much.

Finally, we will hear from Mr. Mike Hintze.

Mr. HINTZE. Hintze.

Senator DORGAN. Mr. Mike Hintze. I am sorry. Mike Hintze is the Associate General Counsel at Microsoft Corporation. Mr. Hintze, you may proceed.

STATEMENT OF MICHAEL D. HINTZE, ASSOCIATE GENERAL COUNSEL, MICROSOFT CORPORATION

Mr. HINTZE. Thank you, Mr. Chairman, for inviting me to testify today about the privacy implications of online advertising. This is a critically important topic that Microsoft takes very seriously, and we applaud the Committee for its leadership in this area.

Online advertising, as you acknowledged, has become the engine that drives the Internet economy. Millions of websites are able to offer content and services for free to consumers because of the revenue they derive from advertising online. In the United States, the amount spent on online advertising already exceeds spending for advertising through radio, magazines, and cable television. It accounted for $21 billion in 2007 and is expected to grow to $50 billion in the next 3 years.

Online advertising has been so successful because it is interactive and can be targeted to users' online activities and other characteristics. This targeting benefits users not only because it enables free services and content they enjoy, but also because they are likely to see more relevant ads. And it benefits advertisers because they can reach users who are more likely to respond to their ads.

Each search, click, and other user action online reveals valuable information about the user's likely interests, and online ads can be automatically tailored to those interests. In general, most data collection online happens in conjunction with a display of ads. This means the entity with the greatest market share and therefore who serves the most ads online will collect the most data about users.

As this Committee recognizes, the collection of user data to serve ads on the Internet has important privacy implications. Microsoft is here today because we have a deep commitment to consumer privacy. We were one of the first companies to appoint a chief privacy officer, an action we took nearly a decade ago, and we currently have over 40 employees who focus on privacy full-time and another 400 throughout the business who focus on privacy as part of their jobs. We have a robust set of internal privacy policies and standards that guide how we do business and how we design our products and services in a way that protects consumer privacy.

With respect to online advertising, we have taken more concrete steps to protect privacy than any of our competitors. Last July, we released Microsoft's Privacy Principles for Live Search and Online Ad Targeting. We are committed to these principles which focus on three core themes: transparency, control, and security. Let me explain how we have put each of these principles into action in ways that go beyond others in the industry.

The first principle is transparency. We post a clear link to our privacy notice on every page of our websites, including the home page, and we have for several years. We also were one of the first companies to develop so-called layered privacy notice, which gives concise and easy-to-understand bullet-point summaries of our practices with links to more detailed information. And our privacy statement is clear about the data we collect and use for online advertising.

The second principle is control. Microsoft enables users to opt out of behavioral ad targeting, but we also give consumers the option to tie their opt-out choice to their Windows online account. Unlike methods used by other companies, this means that even if they delete cookies on their machine, when they sign back in, their opt-out selection will persist. It also means that a single choice can apply across multiple computers they use.

The third principle is security. For Microsoft, this means not only protecting data from unauthorized access, but also designing our systems and processes in ways that minimize their privacy impact from the outset. We create an anonymized identifier for each of our registered users. Search query data and web surfing behavior used for ad targeting is associated with this anonymized identifier. We also irreversibly and completely remove the IP addresses and other identifiers from search queries after 18 months.

We believe that our commitment to these three principles, transparency, control, and security, and more importantly, the steps we have taken to implement them make us the industry leader in online privacy.

These principles also form the basis for our support for comprehensive baseline privacy legislation, supplemented by robust self-regulation. For example, we have advocated a broader self-regulatory framework than that proposed by the FTC, one that is tailored to account for the type of information collected and how it is used. We have also long supported meaningful privacy legislation which, as CDT appropriately notes, can protect consumers without hampering business.

We view these efforts as part of our multi-faceted approach to protecting consumer privacy, which also includes developing technical solutions and educating consumers about how to protect themselves online. In short, at Microsoft, we are prepared to work collaboratively on all these fronts to protect consumer privacy.

Thank you for giving us the opportunity to testify today, and I look forward to answering any questions you may have.

[The prepared statement of Mr. Hintze follows:]

PREPARED STATEMENT OF MICHAEL D. HINTZE, ASSOCIATE GENERAL COUNSEL, MICROSOFT CORPORATION

Chairman Inouye, Vice Chairman Stevens, and honorable Members of the Committee, my name is Michael Hintze, and I am an Associate General Counsel of Microsoft Corporation. Thank you for the opportunity to share Microsoft's views on the important privacy issues presented by advertising on the Internet. We appreciate the initiative that this Committee has taken in holding this hearing, and we are committed to working collaboratively with you, the Federal Trade Commission, consumer groups, and other stakeholders to protect consumers' privacy interests online.

Much is at stake with respect to the issues we will be considering today. Online advertising has become the very fuel that powers the Internet and drives the digital economy. It supports the ability of websites to offer their content and services online; it has created new opportunities for businesses to inform consumers about their products and services; and it allows consumers to receive ads they are more likely to find relevant. Simply stated, the Internet would not be the diverse and useful medium it has become without online advertising.

At the same time, online advertising is unique because it can be tailored automatically to a computer user's online activities and interests. An online ad can be served based on the website a user is visiting, the searches a user is conducting, or a user's past Internet browsing behavior, among other things. In each instance, serving the online advertisement involves the collection of information about consumers' Internet interactions. And this data collection has implications for consumer privacy.

The objective we face is to maintain the growth of online advertising while protecting consumer privacy. This is a commitment Microsoft embraces. We recognize that consumers have high expectations about how we and other Internet companies collect, use, and store their information. Consumers must *trust* that their privacy will be protected. If the Internet industry fails to meet that standard, consumers will make less use of online technologies, which will hurt them and industry alike.

It also could hurt the U.S. economy. E-commerce sales reached $136.4 billion in 2007, an increase of 19 percent from 2006, according to the U.S. Census Bureau.[1] In comparison, total retail sales in 2007 increased only 4 percent from 2006. If consumers feel that Internet companies are not protecting their privacy, the Internet's ability to serve as an engine of economic growth will be threatened. This means that Microsoft, and all companies operating online, must adopt robust privacy practices that build trust with consumers.

[1] U.S. Census Bureau, *Quarterly Retail E-Commerce Sales: 4th Quarter 2007,* Feb. 15, 2008, available at *http://www.census.gov/mrts/www/data/html/07Q4.html.*

Microsoft has a deep and long-standing commitment to consumer privacy. Microsoft was one of the first companies to appoint a chief privacy officer, an action we took nearly a decade ago, and we currently employ over 40 employees who focus on privacy full-time, and another 400 who focus on it as part of their jobs. We have a robust set of internal policies and standards that guide how we do business and how we design our products and services in a way that respects and protects user privacy.[2] And we have made significant investments in privacy in terms of training and by building our privacy standards into our product development and other business processes.

In general, three key principles have guided our approach to privacy issues:

- *Transparency*. We believe consumers should be able to easily understand what information will be collected about them and when. They also should know how such information will be used and whether it will be combined with other information collected from or about them.
- *Control*. We believe consumers should be able to control whether their personal information is made available to others and should have a choice about whether information about their online activities is used to create profiles for targeted advertising.
- *Security*. Consumers and their information should be protected against outside threats and from unwanted disclosure. Data that directly identifies individual consumers, such as name and e-mail address, should not be stored in direct association with search terms or data about Web surfing behavior used to deliver ads online. And strict data retention policies should apply to search data.

Today, I will discuss why we believe these principles are important, how we have put each of these principles into action, and how they underlie Microsoft's approach to privacy in online advertising. But first I would like to provide an overview of how online advertising works, the role that consumer data plays in serving online ads, and the online advertising market.

I. Online Advertising and the Role of User Data

Consumers today are able to access a wealth of information and a growing array of services online for free. Websites can offer this content and these services for free because of the income they receive from advertising.[3] Just as newspapers and TV news programs rely on traditional advertising, online news sites and other commercial websites rely on online advertising for their economic survival. Online advertising is particularly critical for the thousands of smaller websites that do not publish through offline channels and thus depend entirely on the revenue they receive from selling space on their websites to serve ads online. It is also critical for smaller businesses that serve niche markets (*e.g.,* out-of-print books on European history) who rely on online advertising to reach those niche audiences cost-effectively; indeed, many of these businesses could not survive without it.

The importance of online advertising is evident from its growing share of the overall advertising market. It accounted for $21 billion of the market in 2007 and is expected to grow to $50 billion in the next 3 years.[4] In the United States, online advertising spending already exceeds spending for advertising through radio, magazines, and cable television.[5]

One reason for this rapid growth is the ability to target online ads to Internet users. Newspaper, magazine, and television advertisements can, of course, be targeted based on the broad demographics of readers or viewers. But the Internet is interactive, and this interaction yields a wealth of data about users' activities and preferences. Each search, click, and other user action reveals valuable information

---

[2] Some of these standards are set forth in Microsoft's Privacy Principles for Live Search and Online Ad Targeting, attached as Appendix 1.* This document is also available at *http://www.microsoft.com/privacy*. Additionally, Microsoft's Privacy Guidelines for Developing Software Products and Services, which are based on our internal privacy standards, are available at *http://www.microsoft.com/privacy*.

[3] It has become a standard approach to the online economy that there is a value exchange in which companies provide online content and services to consumers without charging a fee and, in return, consumers see advertisements that may be targeted.

[4] *See* Interactive Advertising Bureau, *IAB Internet Advertising Revenue Report,* 7, May 2008, available at *http://www.iab.net/media/file/IAB_PwC_2007_full_year.pdf*; Yankee Group, *Yankee Group Forecasts U.S. Online Advertising Market to Reach $50 Billion By 2011,* Jan. 18, 2008, available at *http://www.yankeegroup.com/pressReleaseDetail.do?actionType=getDetail PressRelease&ID=1805*.

[5] *See* Brian Morrissey, *IAB: Web Ad Spend Tops Cable, Radio,* ADWEEK, May 15, 2008, available at *http://www.adweek.com/aw/content_display/news/digital/e3ibcf6d45fc7a036dff28457a85c838ff1*.

about that user's likely interests. The more information an entity collects, the greater that entity's ability to serve an advertisement that is targeted to the user's interests. This targeting benefits users, not only because it enables the free services and content they enjoy, but also because the ads they see are more likely to be relevant. And it benefits advertisers because users are more likely to respond to their ads.[6]

There are a variety of ways in which data can be collected about users to serve targeted ads on the Internet. Users reveal information about what they are looking for when they search online, and ads can be targeted to their search queries.[7] Advertising networks enter into agreements with websites that allow them to display ads; to deliver and target those ads, data is gathered about the pages users view and the links users click on within those sites.[8] And new business models are emerging where data about users' online activities can be collected through a user's Internet service provider, and ads can be served based on that information. In general, most data collection happens in connection with the display of ads. This means the entity that serves the most ads (search and/or non-search ads) will also collect the most data about users.

II. The Online Advertising Environment

The online advertising ecosystem has undergone significant changes in the past few years. There continue to be millions of websites that display online ads and thousands of advertisers who use online advertising. However, there is a relatively small number of so-called advertising networks, or "middlemen," to bring advertisers and websites together to buy and sell online ad space. And the number of companies playing this intermediary role has decreased significantly in recent months as a result of consolidation in the industry.[9]

This market consolidation impacts the privacy issues we are discussing today in several ways. First, it is important to recognize that in the past, advertising networks typically did not have direct relationships with consumers. Today, however, the major ad networks are owned by entities—such as Microsoft, Google, and Yahoo!—that provide a wide array of Web-based services and, therefore, often have direct relationships with consumers. This increases the potential that data collected through online advertising will be combined with personally identifiable information. While Microsoft has designed its online advertising system to address this concern,[10] no ad network is required to do so.

Further, as noted above, there is a direct connection between the market share of an advertising network or an online search provider and the amount of data collected about a user's online activity. For example, the larger the share of search ads a company delivers, the larger number of users' online search queries it collects and stores. Similarly, the larger the share of non-search ads an advertising network delivers across the Web, the larger number of users' page views it collects and stores, and the more complete picture of individuals' online surfing behavior it is able to

---

[6] It is for this reason advertisers are willing to pay more for targeted ads. For example, although Merrill Lynch has reported that the average cost per 1,000 impressions ("CPM") is $2.50, entities engaged in behavioral targeting have reported average CPMs as high as $10. See Brian Morrissey, *Aim High: Ad Targeting Moves to the Next Level,* ADWEEK, Jan. 21, 2008, available at *http://www.adweek.com/aw/magazine/article_display.jsp?vnu_content_id=1003695822.* Data also shows that 57 percent of 867 search engine advertisers and search engine marketing agencies polled "were willing to spend more on demographic targeting, such as age and gender." Search Engine Marketing Professional Organization, *Online Advertisers Are Bullish on Behavioral Targeting,* May 15, 2008, available at *http://www.sempo.org/news/releases/05-15-08.*

[7] Search ads are selected based on the search term entered by a user and sometimes on data that has been collected about the user, such as the user's history of prior searches. Search ads generally appear either at the top of the search results or along the right-hand side of the page. They often are displayed as text, but they may include graphics as well. Advertisers bid against each other for the right to have their ads appear when a specific search term is entered (known as a "keyword").

[8] These non-search ads are what users see when they visit virtually any site on the Internet other than a search engine site. They can be based on the content of the page the user is viewing (typically referred to as "contextual" ads) or on a profile of a user's activities that has been collected over time (referred to as "behavioral" ads). But in either case, the company serving the ad would log the pages users view—typically in association with a cookie ID from the user's computer and/or an IP address.

[9] Three examples of this are Microsoft's acquisition of aQuantive, Yahoo!'s acquisition of RightMedia and Google's acquisition of DoubleClick. For more information about the key players in the advertising market and the impact of consolidation in the market, see the testimony of Microsoft General Counsel Brad Smith before the Senate Judiciary Committee, available at *http://www.microsoft.com/presspass/exec/bradsmith/09-27googledoubleclick.mspx.*

[10] *See* section III.C below.

amass. Today, Google AdWords is the leading seller of search advertising.[11] Google also has the leading non-search ad network, AdSense. Google recently expanded its reach into non-search by acquiring DoubleClick.[12] By comparison, Microsoft is a relatively small player in search ads, and its reach in non-search advertising is also smaller than Google's.[13] Google's growing dominance in serving online ads means it has access to and collects an unparalleled amount of data about people's online behavior.[14]

There also is a critical relationship between competition and privacy that must not be overlooked in this discussion. Competition ensures companies have an incentive to compete on the basis of the privacy protections they offer. On the other hand, a dominant player who is insulated from competitive pressure has little reason to heed consumer demand for stronger privacy protections and faces no significant competitive pressure from other firms offering superior privacy practices. Indeed, if a dominant player could generate additional profits by diluting its privacy practices, there is a significant risk it may do so. This could bring about a "race to the bottom" on privacy as other companies weaken their privacy practices in an effort to catch up to the market leader.

Yahoo! and Google's recently announced agreement raises important questions in this regard. Under the agreement, Yahoo! will outsource to Google the delivery of ads appearing alongside Yahoo!'s search engine results.[15] This has the potential to give Google, the market leader, further control over the sites and services where ads are served, enabling Google to collect even more data about computer users and potentially to combine that data with the personal information it has on those users.[16] It also will reduce competition in the search advertising market, and thereby weaken Google's incentives to compete on the quality of its privacy practices. Both of these outcomes have implications for consumer privacy.[17]

III. Microsoft's Commitment to Privacy in Online Advertising

Microsoft recognizes the role that data plays in online advertising and the corresponding importance of protecting consumer privacy. To guide our approach to data collection for online advertising, we released Microsoft's Privacy Principles for Live Search and Online Ad Targeting last July.[18] We are deeply committed to these

---

[11] Based on comScore's Core Search Report, in May of this year, 62 percent of searches were performed in the U.S. on Google, amounting to roughly 6.7 billion searches. comScore, *comScore Releases May 2008 U.S. Search Engine Rankings,* June 19, 2008, available at *http://www.comscore.com/press/release.asp?press=2275.* Google also has strategic agreements with AOL and Ask that allow Google to serve ads to those companies' search engine sites. Adding AOL's (4.5 percent) and *Ask.com*'s (4.5 percent) share of the search queries, Google's share rises to 71 percent. *See id.*

[12] Following its acquisition of DoubleClick, Google now serves in the range of 70 percent of all non-search advertisements. *See, e.g., Lots of Reach in Ad . . .*, April 1, 2008, available at *http://battellemedia.com/archives/004356.php*.

[13] Microsoft's Live Search has approximately 8.5 percent of Core Search queries in the United States. comScore, *comScore Releases May 2008 U.S. Search Engine Rankings,* June 19, 2008, available at *http://www.comscore.com/press/release.asp?press=2275.*

[14] Concerns have been raised about this dominance as well as the privacy protections surrounding the enormous amount of information about users' online behavior that this dominance enables. *See, e.g.,* Electronic Privacy Information Center, *Supplemental Materials in Support of Pending Complaint and Request for Injunction, Request for Investigation and for Other Relief,* June 6, 2007, available at *http://epic.org/privacy/ftc/google/supp_060607.pdf* ("The combination of Google (the world's largest Internet search engine) with DoubleClick (the world's largest Internet advertising technology firm) would allow the combined company to become the gatekeeper for Internet content. . . . The detailed profiling of Internet users raises profound issues that concern the right of privacy. . . ."); *see also,* Jaikumar Vijayan, *Google Asked to Add Home Page Link to Privacy Policies*, COMPUTERWORLD, June 3, 2008, available at *http://www.computerworld.com/action/article.do?command=viewArticleBasic&articleId=9092838;* Privacy International, A Race to the Bottom: Privacy Ranking of Internet Service Companies, Sept. 6, 2007, available at *http://www.privacyinternational.org/article.shtml?cmd%5B347%5D=x-347-553961* (We "witnessed an attitude to privacy within Google that at its most blatant is hostile, and at its most benign is ambivalent.").

[15] *See http://www.google.com/intl/en/press/pressrel/20080612_yahoo.html*.

[16] With Google's 71 percent search query share in the U.S. based on its relationship with AOL and Ask.com (see supra fn. 11), in combination with Yahoo's 20.6 percent share of the core search query market, Google will be able to gather information on up to 92 percent of online searches. *See* comScore, *comScore Releases May 2008 U.S. Search Engine Rankings,* June 19, 2008, available at *http://www.comscore.com/press/release.asp?press=2275.*

[17] *See* Jeff Chester, *A Yahoo! & Google Deal Is Anti-Competitive, Raises Privacy Concerns,* May 22, 2008, available at *http://www.democraticmedia.org/jcblog/?p=596.*

[18] See Appendix 1. Microsoft's Privacy Principles for Live Search and Online Ad Targeting are also available at *http://www.microsoft.com/privacy.*

principles, which focus on bringing the benefits of transparency, control and security to the protection of consumers' data and privacy online.

A. Transparency

I want to first touch upon the importance of transparency. Transparency is significant because it provides consumers with an informed understanding of a company's data collection practices, of how their data might be used, and the privacy controls available to users. Without transparency, consumers are unable to evaluate a company's services, to compare the privacy practices of different entities to determine which online products and services they should use, or to exercise the privacy controls that may be available to them. Transparency also helps ensure that when consumers are dealing with a company that has adopted responsible privacy practices, they do not needlessly worry about unfounded privacy concerns, which could prevent them from taking advantage of new technologies.

Transparency is also essential to ensure accountability. Regulators, advocates, journalists and others have an important role in helping to ensure that appropriate privacy practices are being followed. But they can only examine, evaluate and compare practices across the industry if companies are transparent about the data they collect and how they use and protect it.

Transparency is especially important with respect to online advertising. This is because consumers may not understand the types of information that entities collect or log in providing advertisements online. For example, many consumers may not realize that information about the pages they are viewing, the searches they are conducting, or the services they are using may be collected and used to deliver online ads.

For this reason, Microsoft believes that *any* entity that collects or logs *any* information about an individual or computer for the purpose of delivering advertisements online should provide clear notice about its advertising practices. This means posting a conspicuous link on the home page of its website to a privacy statement that sets forth its data collection and use practices related to online advertising. Consumers should not be required to search for a privacy notice; it should be readily available when they visit a website. This obligation should apply to entities that act as ad networks, as well as to websites on which ads appear—whether they display ads on their own or rely on third parties to deliver online advertising.

In addition to being easy to find, the privacy notice must be easy to understand. While many websites have publicly posted a privacy notice, this alone is not enough. Too often, the posted privacy notice is complex, ambiguous and/or full of legalese. These notices make privacy practices more opaque, not more transparent. Instead, short and simple highlights are essential if consumers are to easily understand a company's information practices. It helps avoid the problem of information overload, while enabling consumer awareness.

Finally, to ensure that the consumer can be fully informed, the privacy notice should also describe the website's data collection and use activities in detail. This includes, at a minimum, descriptions of the types of information collected for online advertising; whether this information will be combined with other information collected from or about consumers; and the ways in which such information may be used, including whether any non-aggregate information may be shared with a third party.

Microsoft has embraced these obligations. We post a link to our privacy notice on every page of our websites, including the home page. We also were one of the first companies to develop so-called "layered" privacy notices that give clear and concise bullet-point summaries of our practices in a short notice, with links to the full privacy statement for consumers and others who are interested in more detailed information. And our privacy statement is clear about the data we collect and use for online advertising. Further, we have released more detailed information about our practices, such as a white paper that describes the methods we use to "de-identify" data used for ad targeting.[19] To illustrate our efforts to be transparent about our practices, we have included in Appendix 2* screen shots of the privacy link available on the home page of our Windows Live search service and of our layered privacy notice, including both the short notice and our full online privacy statement.

B. Control

The second core principle Microsoft looks to in protecting our customers' privacy is user control. Consumers should have a choice about how information about their online activities is used, especially when that information can be aggregated across

[19] See section III.C below.

multiple websites or combined with personal information. Microsoft has made consumer control a key component of our practices online.

As an example, Microsoft has recently deployed a robust method to enable users to opt out of behavioral ad targeting. As background, most industry players that offer consumers a choice about having information about their online activities used to serve behaviorally targeted ads do so by offering consumers the ability to place an "opt-out" cookie on their machines. In general, this process works well, but it does have some inherent limitations. For example, opt-out cookies are computer-specific—if a consumer switches computers, he or she will need to specify any opt-out preferences again. Further, if cookies are deleted from the user's PC, that user's opt-out choice is no longer in effect. To address these limitations, Microsoft now gives consumers the option to tie their opt-out choice to their Windows Live ID. This means that even if they delete cookies on their machine, when they sign back in their opt-out selection will persist. It also means that a single choice can apply across multiple computers that they use. This will help ensure that consumers' choices are respected.[20]

Microsoft also has committed to respecting consumers' opt-out choice on all sites where it engages in behavioral advertising. This means that consumers are offered a choice about receiving behaviorally targeted ads across both third-party websites on which Microsoft delivers behaviorally targeted ads, as well as Microsoft's own websites. This is important because consumers reasonably expect that the opt-out choice offered by a company would apply on all websites where that company engages in behavioral advertising practices. This is another example of where we have committed to going beyond standard industry practice to better protect the interests of consumers.

We also recognize it is appropriate that the level of consumer control may vary depending on the data that will be used to serve an online ad. For example, many consumers have serious reservations about the receipt of targeted advertising based on the use of certain categories of personally identifiable information, particularly those that may be considered especially sensitive. Thus, we have proposed that companies should obtain additional levels of consent for the use of such information for behavioral advertising—including affirmative opt-in consent for the use of sensitive personally identifiable information.[21]

C. Security

The third principle we look to in protecting consumers' privacy is that strong, simple, and effective security is needed to strengthen consumers' trust in our products, the Internet, and all information technologies. Security has been fundamental at Microsoft for many years as part of our Trustworthy Computing initiative. And it plays a key role with respect to our online advertising practices.

We have taken a broad approach to protecting the security of computer users with respect to serving ads online. This approach includes implementing technological and procedural protections to help guard the information we maintain. We also have taken steps to educate consumers about ways to protect themselves while online, and we have worked closely with industry members and law enforcement around the world to identify security threats, share best practices, and improve our coordinated response to security issues.

In addition, we have designed our systems and processes in ways that minimize their privacy impact from the outset while simultaneously promoting security. For example, we use a technical method (known as a one-way cryptographic hash) to separate search terms from account holders' personal information, such as name, e-mail address, and phone number, and to keep them separated in a way that prevents them from being easily recombined. We have also relied on this method to ensure that we use only data that does not personally identify individual consumers to serve ads online. As a result of this "de-identification" process, search query data and data about Web surfing behavior used for ad targeting is associated with an anonymized identifier rather than an account identifier that could be used to personally and directly identify a consumer.[22]

Finally, we have implemented strict retention policies with respect to search query data. Our policy is to anonymize all such data after 18 months, which we believe is an appropriate time-frame in our circumstances to enable us to maintain

---

[20] Microsoft's personalized advertising opt-out page is available at *https://choice.live.com/advertisementchoice/Default.aspx*.

[21] See, for example, Microsoft's comments to the Federal Trade Commission's proposed self-regulatory framework for online advertising, included as Appendix 4* and available at *http://www.ftc.gov/os/comments/behavioraladprinciples/080411microsoft.pdf*.

[22] A white paper describing Microsoft's "de-identification" process is attached to these comments as Appendix 3.* It is also available at *http://www.microsoft.com/privacy*.

and improve the security, integrity and quality of our services. We intend to continue to look for ways to reduce this time-frame while addressing security, integrity and quality concerns. In addition, unlike other companies, our anonymization method involves irreversibly removing the *entire* IP address and other cross-session identifiers, such as cookies and other machine identifiers, from search terms. Some companies remove only the last few digits of a consumer's IP address, which means that an individual search query may still be narrowed down to a small number of computers on a network. We think that such partial methods do not fully protect consumer privacy, so we have chosen an approach that renders search terms truly and irreversibly anonymous.

IV. Microsoft's Support for Self-regulation and Privacy Legislation

Microsoft believes that these core principles of transparency, control, and security are critical to protecting consumers' privacy interests online. These principles form the basis for our support of robust self-regulation in the online advertising market and for baseline privacy legislation.

We have been an active participant in self-regulatory efforts. Microsoft has been engaging with the Network Advertising Initiative ("NAI"), a cooperative of online marketing and advertising companies that addresses important privacy and consumer protection issues in emerging media.[23] The NAI is currently in the process of revising its guidelines to address changes in the online advertising industry. The NAI's efforts have been critical to understanding the privacy issues associated with online advertising, and we will continue to work with them as they finalize their draft proposal.

We also filed comments responding to the Federal Trade Commission's request for input on a proposed self-regulatory framework for online advertising. In our comments, we explained the need for a broad self-regulatory approach since all online advertising activities have potential privacy implications and some may be contrary to consumers' expectations. To this end, we proposed a tiered approach to self regulation that is appropriately tailored to account for the types of information being collected and how that information will be used. It would set a baseline set of privacy protections applicable to all online advertising activity and would establish additional obligations for those companies that engage in practices that raise additional privacy concerns. We are attaching a copy of our comments to the FTC for your convenience.[24]

In addition to supporting self-regulatory efforts, we have long advocated for legislation as a component of effective privacy protections. We were one of the first companies to actively call for comprehensive Federal privacy legislation.[25] More recently, we have supported balanced and well-crafted state legislation on privacy in online advertising that would follow the general structure proposed in our FTC comments.[26] And we would be glad to work with the Committee on similar national privacy standards that would protect both privacy and opportunities for innovation in the online advertising industry.

Our support of self regulation in the online advertising market and prudent privacy legislation is only a part of our comprehensive approach to protecting consumer privacy. We will continue to support consumer education efforts to inform users of how to best protect themselves and their information online. And we will persist in our efforts to develop technology tools that promote the principles of transparency, control, and security. In short, we are prepared to work collaboratively on all fronts to maintain the growth of online advertising while fostering consumer trust online.

V. Conclusion

Microsoft recognizes that the protection of consumer privacy is a continuous journey, not a single destination. We can and will continue to develop and implement new privacy practices and protections to bring the benefits of transparency, choice,

---

[23] Atlas, which was part of Microsoft's recent acquisition of aQuantive, was a founding member of NAI.

[24] See Appendix 4. Our comments are also available at *http://www.ftc.gov/os/comments/behavioraladprinciples/080411 microsoft.pdf.*

[25] *See http://www.microsoft.com/presspass/download/features/2005/PrivacyLegislationCall WP.doc.*

[26] A. 9275–C, 2007–2008 Reg. Sess. (N.Y. 2008), available at *http://assembly.state.ny.us/leg/?bn=A09275&sh=t* (imposing minimum notice and choice obligations on certain website publishers and advertising networks); S. 6441–B, 2007–2008 Reg. Sess. (N.Y. 2008), available at *http://assembly.state.ny.us/leg/?bn=S06441&sh=t* (imposing baseline notice, choice, security, and consumer access obligations on certain third-party advertising networks); H.B. 5765, 2008 Gen. Assem., Feb. Sess. (Conn. 2008), available at *http://www.cga.ct.gov/2008/FC/2008HB-05765-R000148-FC.htm* (imposing minimum notice, choice, security, and use limitations on third-party advertising networks).

and security to consumers. Thank you for giving us the opportunity to testify today. We look forward to working with you to ensure consumers' privacy interests are protected as they continue to enjoy the proliferation of free services and information that online advertising supports.

*The information referred to has been retained in Committee files.

Senator DORGAN. Mr. Hintze, thank you very much. I appreciate your testimony.

To my colleagues, I would say time is not our friend this morning. The vote is supposed to start at 11:15, although I am told it may slip. We will probably know shortly. If it starts at 11:30, that means that we would have perhaps until 11:45 before we would have to depart this room.

I will do 5-minute rounds here, and if we finish at 11:45, we will not have to come back. We have five votes in succession, which means we probably would not be able to come back until 1 o'clock. So my hope would be that for the next 45 minutes to an hour, we will all be able to have an opportunity to ask relevant questions.

And I thank very much the witnesses for being here.

I have 100 questions, regrettably. Let me take just 4 and a half or 5 minutes and then call on my colleagues.

First of all, online advertising is helpful and useful in my judgment. I understand that. It helps support the Internet itself, which has some wonderful companies and sites providing useful information services, entertainment. I understand all of that.

The question today is not, as Mr. Crews indicated, are certain kinds of advertising the devil. I think advertising is a necessary component of the Internet and is helpful to consumers. The question is about the collection of information about consumers as they travel the Internet.

And Mr. Dykes, I will ask you the first question. The stories that I have seen about maybe an Internet service provider deciding we are going to allow NebuAd to come in, and whenever anybody does anything on our system, as someone who has signed up for our Internet service provider service, we are going to essentially shovel all that information over to you as it is being done. I mean, what is the difference between that and tapping into somebody's wire, using the pejorative term "wiretapping"? Is that not just wiretapping?

Mr. DYKES. No, sir. We believe that we are not violating the wiretap law. I am not a lawyer, but my lawyers have told me we are in compliance with the law, and they have prepared a memo on the subject and I would be prepared to submit that for the record. [The information requested is published on pp. 101–107 of this transcript.]

But it is important to note that the information that we are looking at as people surf the web does not involve any personally identifiable information. All we are doing is taking an anonymous identifier. We are taking their IP address, for example, and transforming that into an anonymous number with a one-way hash. And against that anonymous identifier all we are examining is qualification for market segments. So we are not keeping the raw data. It is just qualification for market segments against an anonymous identifier.

Senator DORGAN. But your approach and the approach of the Internet service provider would not be an opt-in approach. It would be an opt-out approach. I would think if my Internet service provider said to me, you know what, Mr. Dorgan? We have a proposition. Is it OK if we give everything you do to another company? I would say, of course, it is not OK. You kidding me? The answer is no, capital N-O. So from an opt-in standpoint, I am guessing that this would not be a workable model. It only works if you require people to opt-out. I mean, I think that is the difficulty.

Ms. Harris, do you want to comment on that?

Ms. HARRIS. Yes, I do. I think, first of all, it is important to understand that our wiretap laws do not care if the information is personally identifiable or not personally identifiable. The laws are agnostic on that point. It is important to understand that.

Second, they may not be using all the information, but they are mirroring. They are capturing the data stream and then somehow mirroring or copying it. So the ISPs are providing that information to an unknown third party, a man in the middle. I take Mr. Dykes' word that they are then not using all of that information, but you have to have a way to separate out the information you are using from the information you are not using. I do not think you can pretend——

Senator DORGAN. Mr. Dykes, do you wish to respond to that?

Mr. DYKES. Yes, I would, Mr. Chairman. So although the information flows through our system, information that does not conform to one of the market segments we are looking at is simply ignored and flushed permanently. And so we are only looking at these select innocuous market segments.

I would also point out that we do provide very robust notice to the user and an opportunity to opt out. These notices are sufficiently robust that people do opt out. So it is not like people are ignoring them. They are informed, and as I said, we are confident that we do not break the law and we have a memo on the subject that we would submit.

Senator DORGAN. Mr. Kelly, on Facebook, I do not know whether this has changed, but my understanding is that when someone would order an application, which they could on Facebook, called Dogbook or Scrabble, that that application then would allow the person selling the application access to all that which exists in Facebook. Was that the case?

Mr. KELLY. So, first of all, a user has to affirmatively add an application to a profile and——

Senator DORGAN. I understand, but when they do that——

Mr. KELLY.—box that informs them that they are adding this application and sharing information with the third party in that case. At that point, the application has the ability to request certain data. We do not hand over all the data at that point. They have the ability to request it in a session basis and limit it to the data that the user who has installed the application can see on Facebook. So the privacy settings persist.

That application is allowed to, for caching purposes, retain the information they have requested for only 24 hours, and if they exceed that amount, we have a policy enforcement team which will take action, including potentially shutting down the application.

And in the last few weeks, we have shut down a number of applications over violations until they come into compliance.

Senator DORGAN. I have just received some good news. The U.S. Senate was not constructed to ever be accused of speeding, and all of us who serve here know that. It actually has exhibited that this morning. We have actually an 11:45 start time, which means we have a full hour for questions. The 11:45 start time will be the first vote. So that is good news.

Let me call on Senator Vitter.

STATEMENT OF HON. DAVID VITTER,
U.S. SENATOR FROM LOUISIANA

Senator VITTER. Thank you, Mr. Chairman. I have some general questions and I would invite very concise responses from anyone who has a response.

What is the best estimate available regarding the use of this type of information not for behavioral advertising—put that on the side—but for other purposes that all of us would consider an abuse, identity theft or other abusive uses, not behavioral advertising? Does anyone have a sense of the size of that problem?

Ms. HARRIS. Mr. Vitter, I think that the answer is nobody knows and there are no rules in place that would prevent any of that. And so the question is, and I will say that for members of the Network Advertising Initiative that they have made a commitment not to do that, but it is a big Internet. And we do not know what everybody is doing. But basic fair information practices say that if you collect information for a purpose, you should use it for that purpose, and not use it for another purpose. We have no legal way of enforcing that.

Senator VITTER. Does anyone else have a sense of the size of that problem?

Mr. DYKES. Well, I would point out that when NebuAd was being founded back in 2006, it was when AOL search data became public and people determined that a large amount of raw search data could represent personally identifiable information. We also had the Government asking Verizon and AT&T to provide click stream data.

And it was for those reasons that when NebuAd was founded, we resolved never to be in a position to have such data that, which if found by others, could ever have a problem. That is why we do not keep the raw data mapped against a user ID. We only keep this qualification for market segments and all our user ID's are anonymized. So we keep very limited data to avoid any of those risks.

Senator VITTER. I understand.

Does anyone else have a sense of the global size of that problem? OK.

Now, with regard to that problem—again, put behavioral advertising on the side. With regard to that problem, would ensuring that all of this collection of data is made anonymous in the ways that several of you do presumably already solve that problem or not?

Ms. HARRIS. I do not think you can do that. The industry wants us to believe that this information is anonymous. I think at best

it is pseudo-anonymous. They are building profiles. And I think a couple of years ago when AOL released search data for a good purpose, for research purposes, it took very little time for people to take a single set of search data and identify somebody. So that we are moving to a point where there is enough information——

Senator VITTER. Can I interrupt for a second?

Ms. HARRIS. Yes.

Senator VITTER. Explain that to me as a layperson because my reaction to that is there are a gazillion people on the Internet. How do you possibly take that anonymous information and come up with an individual?

Ms. HARRIS. Well, it cannot be entirely anonymous because you are trying to put—I mean, even for NebuAd—and we can talk about this—they keep refreshing the information about an individual. You have to. Right?

Mr. DYKES. We only keep information in market segments. The way AOL's data became identifiable is that people did numerous searches on houses in their neighborhood, and soon it was fairly clear who the person was who was doing the search because there was just so much data centered on a particular name and address and things like that.

Ms. HARRIS. But profiles can include that. Profiles can include that you have been on a particular website looking at a particular thing, that you have searched for your own name, that you—it depends what is in the profile.

Mr. DYKES. Exactly. If the profiles had that information, that is when it becomes pseudo-anonymous, and therefore, you can derive PII.

Senator VITTER. Let me reask the question. Could there be a regime ensuring true anonymity in terms of the collection, number one? Is that possible?

Mr. DYKES. I believe so.

Senator VITTER. And number two, is any legitimate purpose that is of any arguable benefit to consumers sacrificed through that regime?

Mr. DYKES. Well, the effectiveness does decline as you move toward eliminating pseudo-anonymous data. But we have chosen to make that choice. We do not have very sensitive ads. We have chosen not to take very sensitive ads from big pharmaceutical companies, for example. There are a lot of choices we have made to protect consumer choices that do reduce the economic value, but these I think are important choices.

Senator VITTER. Does anyone else have a reaction to that idea of what most folks would regard as true anonymity? Number one, how possible it is; number two, what if anything would be sacrificed.

Mr. CREWS. I think you are always taking a risk when you think that the Internet, with the kind of network that it is—if pure privacy is what you want, the Internet is probably the wrong network for you because everybody here has a business card, and the people that we talk about with most of these new technologies—and I talked about warring computer scientists. Some are trying to offer anonymity.

But on the other hand, there are going to be cases where you do not want somebody to pose as you and you are going to want to use personally identifiable information. The technologies are going to change as biometrics get integrated into commerce and things like that. So we are not going to want anonymity ultimately in some respects, if we are dealing with our insurance company, dealing with a finance company.

Senator VITTER. Let me back up. I am not talking about anonymity dealing with your insurance company. I am talking about anonymity in terms of the collection of data for the purposes that we are talking about.

Mr. CREWS. I do not think so because of the openness of the Internet and the criminal element that is always going to be there. You know, anybody can go into Starbucks and the library and get on the Net. It is always going to be an open network that nobody has a proprietary stake and can offer that kind of a guarantee. We are going to have to have activities on the consumer side and institutions like identity theft insurance and all those sorts of things too. We can try our best, and I think that is what scientists are trying to do. But the Internet is not the network for privacy in a sense.

Senator VITTER. Thank you.

Senator DORGAN. Senator Stevens was here and he had to go to an Appropriations Committee markup, and he asked that we put his statement in the record. We will do that by unanimous consent.

[The prepared statement of Senator Stevens follows:]

PREPARED STATEMENT OF HON. TED STEVENS, U.S. SENATOR FROM ALASKA

Mr. Chairman, thank you for scheduling this hearing.

As we recently learned in last month's hearing on spyware, we must be increasingly vigilant in ensuring that Americans' personally identifiable information is protected. On one hand, legitimate online advertising provides many benefits to our economy—for example in Alaska it helps our newspapers, radio stations and television stations to provide free online news. But, on the other hand there are concerns about protecting individuals' privacy and preventing against identity theft.

For the Internet economy to continue to grow, Americans need to have confidence that their personal identifiable information is safe when they enter their data online. Moreover, consumers should be fully informed about what information is being collected online, who is collecting the data, and what options consumers have to protect themselves.

At this hearing, it will be important that the Committee gets a sense of how online behavioral advertising works, and how consumers can guard their personally identifiable information. I also anticipate that today's hearing will help us better understand what roles the Federal Trade Commission and the industry should play in educating consumers on how information is collected online and how to protect themselves.

I thank the witnesses for participating today and look forward to hearing their testimony.

Senator DORGAN. Senator Klobuchar?

STATEMENT OF HON. AMY KLOBUCHAR, U.S. SENATOR FROM MINNESOTA

Senator KLOBUCHAR. Thank you very much, Senator Dorgan, for holding this hearing, and thank you to our witnesses. I was thinking, as I listened, how everyone sort of has a love-hate relationship with advertising on the Internet. I love it when it is something for a discount on clothes, and I hate it when my daughter sees the

American Girl things put on the screen. But I think everyone feels like that.

And I think we also know that advertising plays an important role in enhancing a consumer's online experience. It is revenue, and it also promotes the development of online news. So like Senator Dorgan, I would agree that we are not against advertising on the Internet, but the issue is, as it becomes more sophisticated, do we have a role here to play in making sure that consumers' privacy is protected as companies develop more technology and are able to dig deeper into that information, that we keep it anonymous.

I guess my first questions are of you, Ms. Parnes. I know Mr. Kelly and Mr. Hintze were talking about how the FTC could go farther in terms of differentiating between the kind of information, whether it is anonymous information, whether it is—I think they were differentiating between the way you get the information based on personally identifiable information or advertising based on non-personally identifiable information. Could you do that as part of your rules?

Ms. PARNES. Well, Senator, I think we could make those distinctions. In the first instance, let me just clarify that what the Commission put out was a set of proposed principles that would guide——

Senator KLOBUCHAR. Self-regulation.

Ms. PARNES.—a self-regulatory scheme.

Senator KLOBUCHAR. Right. They were not rules.

Ms. PARNES. Not Commission rules.

But within the the principles, I think our proposal reflects some differences. For example, the proposal calls for express affirmative consent before an entity can collect sensitive personal information from a consumer for use in behavioral advertising. So we acknowledge that there are some areas that are more sensitive and that require a certain level of heightened transparency and control and choice for consumers. I think that as we are looking at all the comments that we received, that is certainly something that we will consider, whether we should provide a sliding scale type of scheme.

Senator KLOBUCHAR. The other thing is I know you have had 60 comments, and I am sure a lot of them have been industry groups and privacy groups. But again, as Senator Dorgan was mentioning, I am not sure individuals out there even understand what is going on.

I was reading about the European Union has some guidelines where you have to be able to access what people have on you and then correct it if it is false. Have you looked at that at all?

Ms. PARNES. In these sets of principles, we have not looked at access to the information. I think what we have been more concerned about is the issue of transparency, consumers really understanding what is going on in behavioral advertising.

I frankly was surprised that among the over 60 comments we received, we did get some comments from individual consumers, but I think that you are absolutely right. For the most part, consumers do not understand what is happening behind the screen, as it were.

Senator KLOBUCHAR. Mr. Hintze, you talked about the need for a Federal law, and I think Ms. Harris talked about updating Fed-

eral laws. What ideas do you have for changing Federal law that we could look at?

Mr. HINTZE. Well, going back a couple of years to 2005, we came out in support of a comprehensive Federal privacy legislation. We think that establishing a baseline at the Federal level across industries makes a lot of sense. It would require certain basic requirements that are consistent with good industry practices and self-regulation that exists today around user notice and security and user consent and even access, as you have mentioned. There are some very difficult issues there. We have some ideas of what a good Federal law might look like.

We have also been supportive of State legislation in some cases where it was balanced and provided appropriate guidelines for the online advertising space. We have also been very supportive of the security breach notification laws and others.

But I think that overall, legislation does play an appropriate part of the mix of protecting consumer privacy along with self-regulation and consumer education and technology tools.

Senator KLOBUCHAR. So the idea would be to take some of the things that Ms. Horvath has been talking about, some of these other things and actually put them into law. How would it work with the self-regulation?

Mr. HINTZE. Well, the Federal law would presumably provide a baseline common set of requirements, and then for particular industries, for example, there may be additional very specific self-regulatory additions that could go on top of that. I think online advertising is a perfect example of that where there are some specific aspects of online advertising around behavioral targeting and what consent looks like in those cases. That may be more appropriate for self-regulation, but could certainly build on top of the baseline requirement that is based in law.

Senator KLOBUCHAR. Mr. Kelly, did you want to add, since you raised that issue of different ways that we could differentiate between information? Are you in favor of some kind of Federal law?

Mr. KELLY. We have not taken a position on a formal Federal law around that. We have been focused on creating innovative privacy technology to allow users to control the collection and use of data. An instructive example here would be that, for instance, in a classic behavioral targeting situation, an ad network would see that you visited five auto sites and determine from that that you might be interested in buying a car. Whereas, the Facebook approach has been, let us say, if we were, for instance, partnered with an auto site, the auto site would allow you to say—you know, give you a little pop-up that said, do you want to share the fact that you purchased a Chevy with your Facebook friends, and give you a real-time choice around that. So we are focusing on technology as a solution.

Senator KLOBUCHAR. Thank you very much.

Senator DORGAN. Senator Klobuchar, thank you very much.

Senator DeMint?

STATEMENT OF HON. JIM DEMINT,
U.S. SENATOR FROM SOUTH CAROLINA

Senator DEMINT. Thank you, Mr. Chairman. Thank you for holding the hearing. I appreciate your comments on the importance of advertising. I think we all agree that the ability to get all the free things we get on the Internet are important, and they do relate directly to advertising. And I think probably most of us would agree that the ability of advertisers to target their markets are important to continue to attract advertising revenue to the Internet, and I think we have heard a lot about how the industry has progressed.

Just a couple of questions here. Mr. Dykes, just as a for instance so I can kind of get it, this anonymous versus not anonymous question, if the Department of Justice were to issue you a subpoena asking you for names of people who have searched for information about explosives, would you be able to provide the names or locations of individuals who had done that?

Mr. DYKES. No, sir, we would not be able to provide names, nor even their IP addresses. We have no personally identifiable information in our system, and it would just simply not be possible to get back to an individual from any information we have in our system.

Furthermore, we do not have advertisements and categories on bomb-making, for example, and therefore, that information is not even in our system either.

Senator DEMINT. So it appears that the technology has been developed and is being developed and improved that would allow increasing privacy and anonymity on the Internet, which is I think impressive, given the fact that this is all being done voluntarily.

It would be my assumption that the incentives for—the businesses represented at the table have a lot of incentives to compete for the best privacy policies, that they would disclose their privacy policies to encourage users to use their particular service because of their ability to protect. I think the private market has a lot of incentives.

Let me just direct a few questions at Ms. Parnes. How long do you think the rulemaking or even the development of these principles might take?

Ms. PARNES. Well, I am reluctant to give a specific time-frame, but we are moving quickly on this. As we noted, we received a lot of comments, and this is a challenging issue. We want to drill down, figure out what information we have, if we need additional information, and then move forward, as I said, very quickly.

Senator DEMINT. Do you think at least a year or 2?

Ms. PARNES. I would doubt that.

Senator DEMINT. Do you think it is the responsibility of the FTC to regulate advertising on the Internet?

Ms. PARNES. Well, in some ways we do regulate advertising on the Internet. The question about behavioral advertising—I think some of our principles are grounded in section 5, and we do have principles that govern behavioral advertising, as well as all other advertising.

Senator DEMINT. It would be my hope that you continue to see your responsibility as protecting consumers and not necessarily attempting to manage or regulate different aspects of our economy.

I think in some ways we have got a solution in search of a problem, as the industry moves very quickly to try to cut these problems off before they occur. It is very likely that if rulemaking or even principle-making is going to take a year or 2—and obviously, the FTC needs to look at it—that the technology that is being talked about today will advance—will make great strides over the next months and years. And it is very likely that by the time the FTC acts, that the industry will be far ahead of where you are.

My concern is this. The Government's attempt at privacy certainly is well motivated, but rules, for instance, in the health care industry where, when I was with a family member having surgery, the physician was not able to give me information about actually what took place or I could not call a doctor's office and get information about my own daughter's bill. And you hear doctors talk about the inefficiencies that are created because of this well intended policy. I just have great concerns that if the Federal Government attempts to jump in in the middle of a situation where a problem has not yet exhibited itself, that we are likely to inhibit one of the showcases of free enterprise in America today.

Ms. PARNES. Senator, I would just say that that is precisely why the Commission is encouraging self-regulation in this area. The principles that we have proposed are principles that would govern a self-regulatory scheme that industry itself adopts, and we think that self-regulation, at least at this point, is more appropriate in this kind of environment where, as you note, technology is changing so quickly.

Senator DEMINT. Well, that is a good philosophy, and I appreciate hearing it this morning. And I thank all the panelists.

Mr. Chairman, I yield back.

Senator DORGAN. Senator DeMint, thank you very much.

Senator Thune?

STATEMENT OF HON. JOHN THUNE,
U.S. SENATOR FROM SOUTH DAKOTA

Senator THUNE. Thank you, Mr. Chairman. I too want to thank you for holding the hearing. I think this is an issue that is very important. It is being talked about, getting a lot of attention. It is going to get more attention, I think, in the future. I do believe that it is critical that consumers have knowledge of whom or what is tracking their online activity and additionally that they have every opportunity to learn more about the uses of their personal information.

In that light, I have a question for Ms. Parnes, and that has to do with sensitive information which certainly, I believe, would deserve a greater degree of protection than just regular online uses. What do you consider to be sensitive personal information? Is that a health record, a credit card history, those sorts of things?

Ms. PARNES. In our proposal, we identified several examples: medical information, financial information, and any information about children. It is not intended to be an exclusive list, though.

Senator THUNE. What is the relationship between market share in the search advertising business and the ability to attract advertisers and web publishers? And is there a tipping point where a company, for example, say a Google, could become so dominant in

the market that advertisers and web publishers have no choice but to contract with the company?

Ms. PARNES. I am afraid that——

Senator THUNE. Of venturing into that?

Ms. PARNES.—I do not think I really have the information. Yes. It would be difficult to venture a guess on that. Perhaps one of the people here might want to.

Senator THUNE. All right. We will let you off the hook, but if anybody else would care to take a stab at that.

Mr. CREWS. Well, I do not think you have to worry so much about tipping points in the online world for a lot of reasons, but in particular, as long as people have the ability to click that button and there is no censorship online—you know, Government does not dictate where we go or anything like that—no one can attain that kind of monopoly power because nobody operates in a vacuum.

The joke way I put it when debating media ownership is that even if the biggest companies merge with others across other avenues, what happens? They could get together and try to abuse the trust or what have you. But what happens? Advertisers flee. Wall Street flees. Customers flee. The employees flee. The people who work in that business who know the technology and the science move and start another company.

So all of the impulses in a market economy, especially in one where barriers to entry are so low, like in Internet businesses, there is not that kind of threat of monopoly power. It was not that long ago that all of us were using Yahoo! to search or Alta Vista to search, and then Google came along with another technology. It is one algorithm, but you can go on the search engine Colossus I believe. There are hundreds of search engines out there. Just a thought.

Senator THUNE. If Congress were to establish regulatory guidelines or core principles for online advertising privacy, what would those principles entail, and how would those align with some of the principles that the FTC is adopting? Does anybody want to venture——

Ms. HARRIS. Yes. Mr. Thune, I think it is important to note CDT's position in support of a baseline privacy law is not about advertising. It is a step down. It is for all data collection and use practices. So those of us who are advocating adoption, I think you are looking at fair information practices. You collect for a particular use. You hold it only for the time that use exists. You do not hold data forever. People have a right to know what people are holding about them. They have a right to opt out or opt in, depending on the sensitivity of the data. The the devil here is in the details, but I do not think that the framework—you know, fair information practices is sort of infused throughout our legal system and certainly in terms of Government information, although somewhat outdated.

Let me just add one thing. We do understand and have no interest in slowing down the technological innovation in terms of privacy-enhancing technologies. We do think that that is an important part of this, and we would not want to see any law that froze the Internet in a way that would make that impossible. So everything is a balance here.

Mr. HINTZE. I think that is right. We generally agree, and one of the reasons that we came out in favor of comprehensive Federal privacy legislation in 2005, which was before we were significantly involved in the online advertising space at all, is that there is just this emerging patchwork of Federal and State privacy laws with different standards depending on the industry, depending on the particular issue. And it just made a lot of sense to harmonize that, both from a compliance standpoint from a company's point of view and from a consumer standpoint so they can know that they have a common baseline protection across the board, regardless of the kind of industry that they are dealing with.

As we get into online advertising, that kind of baseline Federal privacy standard could certainly help here. It does not answer all the questions, and that is why we need to supplement it with self-regulation and other practices. But I think the need for a Federal law is not specific to online advertising but is more general.

And I would just like to make one other point about your other question earlier about the competition and dominance in this space. I think for the purposes of this hearing, we definitely see a nexus between competition and privacy in that if there does become a dominant player in the online advertising space, that means that there is a single company that is collecting more data. The more ads you serve, the more data you are collecting. And it could become the case where a single company has a nearly complete picture of people's online behavior.

Beyond that, we also think that the need for competition in the space fosters competition in privacy. If there is a dominant player, there is little or no incentive to adopt better privacy practices because they are not facing competitive pressure from other companies that may be adopting superior privacy practices.

Mr. DYKES. Senator, I would like to agree with both of the prior speakers. I think the law should be focused on privacy and what types of information are being collected. And they should be technology-neutral and business process-neutral and not necessarily advertising-focused either. It should really be focused on privacy.

But I also think that the Government needs to be very careful in making policy to ensure that it does not stifle competition for the very reasons we just noted because there are new competitors springing up all the time. When we think we have one dominant competitor, past history has shown that there are other ones in the wings springing to life, and we would not want the Government to stifle that. So there is a role here for self-regulation as well to allow for flexibility as technology develops.

Ms. HARRIS. Can I just make one brief point on this notion of technology neutrality in the law? We do have neutrality under ECPA. If you are acting as a conduit, you are treated one way. If you are not you are treated the other. And I think we have to be careful. We have wiretap laws. We have other communications laws that apply to the institutions that stand between the user and the ends of the network. I think we can sort of use this neutrality—everybody should be treated the same at all times—as a mantra and lose, I think, track of the fact that companies stand in different positions to a consumer, and we have to take that into account.

Senator THUNE. Thank you all for your testimony.
Thank you, Mr. Chairman.
Senator DORGAN. Senator Thune, thank you.
Senator Nelson?

STATEMENT OF HON. BILL NELSON,
U.S. SENATOR FROM FLORIDA

Senator NELSON. Mr. Chairman, I think the timing of this hearing is uncanny because we have on the floor right now the FISA bill which the whole question in FISA is about the protection of the rights of privacy and the civil liberty of Americans. I can tell you all that as a member of the Intelligence Committee, we have been struggling with this FISA issue for the last year and a half. We have come up with a compromise and a resolution of how you can allow our intelligence agencies to seek the information of a terrorist but at the same time protect the civil liberties of American persons, which is defined as an American citizen and a person not an American citizen who is legally within the United States.

What I am struck with is that we have a similar issue here. Take, for example, I use the Internet to go online to read the newspapers back home in Florida. Now, if suddenly the kinds of articles that I am reading are going to be determined, the content of what I am reading is going to be identified with me so someone can target advertising, I want to question the underlying basis of this.

In our discussion of snooping of terrorists before, we have carved out an exception that we do not want the Government—now, here we are talking about the private sector, but we do not want the Government sector to go and examine what books that we are reading at the local libraries. Well, right here we have the question of whether or not we are going to let other private people within the private sector examine the same thing and then use it for a commercial advantage.

Now, I am not naïve enough not to understand that this is already happening. So the question is, how do we rein this in so that as this Internet continues to explode into something years down the road that we cannot even conceive now that will be totally ubiquitous, how do we support our Constitution and protect our civil rights?

So let me just ask, is there a way that we can approach this where we would govern the type of Internet connection used instead of the content or the information collected? What do you think about that, Ms. Harris?

Ms. HARRIS. Well, I think I am not entirely sure of what you are suggesting, Senator.

Senator NELSON. Nor am I.

[Laughter.]

Ms. HARRIS. Well, I am not sure that that is really the answer.

I will say this, that you are, I think, very prescient to connect what appears to be a totally unrelated matter of FISA with what is going on here. And the reason is that when we operate in an Internet regime where we have no limits on how long a company can collect data, where we have these other sets of laws, you know, the Electronic Communications Privacy Act, et cetera, that are 20 years old and did not anticipate the Internet. Whatever we are

building here and whatever is being collected, to the extent that it can be pseudo-anonymously connected through user logs, et cetera, it is also available to the Government. So I do not think we can view these things as there is a consumer stream that is being collected out here and there is a Government stream.

If you look at e-mail, for example, we have very little protection in this country for stored e-mail because we did not anticipate 20 years ago that it was going to be stored online. That information has very little legal protection. So we are in a perfect storm——

Senator NELSON. Yes, we are.

Ms. HARRIS.—between the commercial activity and national security——

Senator NELSON. Yes, just like—you know, we hold it very dear in this country that we do not like other private citizens reading our personal mail, but in effect, what we have is the ability to read our personal communications here by other private individuals separating the issue from Big Brother and the Government.

Ms. HARRIS. I do not think you can.

Senator NELSON. Well, let me ask you this, Ms. Harris.

Ms. HARRIS. That is not to suggest that they are acting as agents for the Government. I want to be really clear here. It is just that the laws we have, once we collect this data——

Senator NELSON. But they could act—that information could, but I do not want to get off on that tangent.

Let me ask you this, Ms. Harris. Do you believe consumers are entitled to an opt-in arrangement rather than the opt-out?

Ms. HARRIS. I think it depends on the data and I think it depends on the context.

Senator NELSON. Give me an example.

Ms. HARRIS. Well, I think that we think that when you are operating in an environment where you are the ISP and you are standing between the ends of the network, that we already have law, the Electronic Communications Privacy law, Cable Act, and a myriad of State laws, that require an opt-in. The ISP stands as sort of the center of Internet chain of trust between the two ends.

And so online in the advertising context, if we could figure out a robust way to do opt-in, but then where we have difficulty is separating PII and non-PII, personal information is starting to merge. It is much harder to separate them. We have profiles of what seemingly each piece looks like, you know, an innocuous piece of information, and they are tied to some kind of ID so they can be refreshed, and that ID can be tied to your Internet address. It is a very complicated area.

That is why I am really pleased to hear Senator Dorgan talk about more hearings. I think we have to get a baseline privacy bill, but we are going to have to do a lot of work to go through——

Senator NELSON. I want to commend Senator Dorgan for doing this, and this is the beginning of a long road as we try to grapple with this issue.

May I ask one more question?

Senator DORGAN. Yes. Your time is expired but we will recognize you for one more question. We are going to have a second round because we have until 11:45. So you may proceed.

Senator NELSON. Right now we have got the Commission doing this self-regulatory principle and it deals with the internal information security, but it may not address the security of these third parties. I wanted to ask you, Ms. Parnes, has the Commission studied the types of data security or encryption associated with these activities?

Ms. PARNES. The Commission has not specifically studied whether all of this information that is being collected is encrypted, but one of the principles that we have announced calls for data security so that the information that is collected is held in a secure way. And we have also called for information to be held only as long as it is needed for some legitimate business or law enforcement purpose. We do not focus particularly on encryption or any other type of technology in looking at data security. It is reasonable security measures in light of the nature of the information that is held.

Senator NELSON. Thank you.

Senator DORGAN. Senator Nelson, thank you very much.

Let me make a couple of comments then ask some additional questions. To give you an example of, as a consumer, things that I think are beneficial in terms of online collection of information, I go to—maybe I should not use the site name—Amazon as an example and am searching for a book or a couple books. And Amazon comes back to me and says here is what you searched for previously. So all of a sudden, I know they have kept information about me. Correct? And then they also come back and they say, and by the way, here are other books that people are looking at when they look at the book you are—so they are obviously collecting information about what other people have done. Very beneficial and very interesting to me to take a look at that. I do not walk away from that computer thinking, you know, that is a real serious problem. I think that is an advantage.

But then there are other questions. For example, Ms. Horvath, Google. I use Google as a verb because I just google it. I am always googling something. Right? And so is Senator DeMint I will bet. And I also use MSN. So the two of you, Google and MSN, likely have information about where I have been traveling. Right?

I did not do this. So I go to—well, I may not google this, but I may. I decide I am going to get to WebMD somehow or another and I am going to take a look at gout, dementia, and postnasal drip. Right? Now, I do not want the whole room to know that, not that I would do that.

[Laughter.]

Senator DORGAN. But that may apply to some others, but I disavow it.

But my point is I do that and then I say, I want to find a flight to San Francisco. I want to go to the St. Francis Hotel, and then I want to go to a Flying Other Brothers concert. So I am doing all that.

So now both of you perhaps know all of that about me or maybe that was all Senator DeMint that did that. So let me ask you a question. Do you know that about me?

Ms. HORVATH. Actually we do not. It would really depend on how you are using our service.

Senator DORGAN. Well, let us say I use it so that you know it.

Ms. HORVATH. If you are signed-on account holder, if you are signed in, then we would know what you are searching for, but we know what you are doing only on the *Google.com* site. Once you leave the *Google.com* site, the connection is gone. We are not collecting——

Senator DORGAN. If I am on MSN and pull up Goggle on MSN and use Google to go find something, you are saying that you do not keep a record of that?

Ms. HORVATH. We would know what your search query was.

Senator DORGAN. Right.

Ms. HORVATH. If you came onto our service to *Goggle.com* and you were not logged in, what we would collect would be your IP address, the operating system that you are using, the browser type that you are using, the query that you have requested, and we would, if you do not have a correct cookie already——

Senator DORGAN. That was my point.

Ms. HORVATH.—we would have a cookie.

Senator DORGAN. That was my point.

Ms. HORVATH. And that is all we would collect.

Senator DORGAN. Well, that is a lot.

Ms. HORVATH. If you went out to the airline site——

Senator DORGAN. You know about postnasal drip then. Right?

Ms. HORVATH. No.

Senator DORGAN. You do not know that is where I went?

Ms. HORVATH. But if you were searching on Google for postnasal drip, we would know that you were searching for that, but once you went off——

Senator DORGAN. Right. That is my point.

Ms. HORVATH.—to WebMD, we would not know that you were searching for gout or——

Senator DORGAN. So how long do you keep the postnasal drip inquiry?

Ms. HORVATH. Well, it is only connected to your IP address. There is an argument as to whether IP addresses are personally identifiable information because of the nonstatic nature. When you are assigned an IP address, it does not mean that you are going to have it 3 days from now, the same IP address. So it would be stored in our logs iteratively. So it would not be saying Senator Dorgan was looking for postnasal drip in our logs. No, we would not know that.

Senator DORGAN. I am using a silly example, obviously.

Ms. HORVATH. No, I understand.

Senator DORGAN. But if I am on MSN, as an example, and I am moving around, and then I go to Google and type in dementia, MSN has a record of what I am doing, I assume, and you have a record of what I am doing at Google. My question is, how long do you keep those records?

Ms. HORVATH. We store our search logs for 18 months, and after 18 months, we anonymize them by deleting what would be your cookie ID and also by redacting the IP address so it could no longer be connected to a computer that you used.

Senator DORGAN. And how long do you store this information?

Mr. HINTZE. Ours is 18 months as well and our anonymization process goes a little bit further. We delete the entirety of the IP address and all cookie ID's.

Senator DORGAN. And if you are a Gmail user and log in, then what?

Ms. HORVATH. Then the logs are exactly the same. It is 18 months and then it is deleted after that.

Senator DORGAN. And if Mr. Dykes comes to you at Google or MSN some day and says, I want to contract with you all, or goes to Verizon or whomever, a service provider or an online company, and says, I would like to contract, I would like to get everything that you have got, just stream it over to me, because he is an advertising agency and he is going to frame up advertising in the future that will have beneficial content for somebody, your reaction to that? He says, I can actually pay you some pretty big money if you just stream all your stuff to me at the same time you are collecting it.

Mr. HINTZE. It is a hypothetical. We would, obviously, look at all the privacy implications of any deal we would do. Currently we are not sharing that data with anybody. It is all used for our own internal operations. As far as I am aware, that is our plan going forward.

Senator DORGAN. Yes, Mr. Dykes?

Mr. DYKES. I would point out that if we were involved in that type of transaction, we would not be storing the sensitive medical information that you just cited, and we would not have the IP address because we do a one-way hash on that. So we would just keep it against an anonymous identifier the innocuous commercial categories that occurred there.

Senator DORGAN. I understand.

Ms. Harris, Senator DeMint, my colleague, indicated—and I think Mr. Crews also—that this is probably a solution in search of a problem, this discussion. And Mr. Crews' point, I think is that if somebody is doing something you do not like, you are going to go someplace else. If you back all the way up from that, that is like you do not need FDA inspecting food plants because if somebody is producing food that makes you sick, they will be out of business soon. But I mean, some make that point that are really against all regulation. But is this a solution in search of a problem?

Ms. HARRIS. No, I do not think it is. You would have to have a level of transparency. And believe me, we encourage every day our colleagues at this table and some who are not and industry to compete with each other on privacy. But I do not think consumers understand at a level of granularity about the differences in policies. And I can say you are still keeping information far too long. We still have information tied to IP logs. I mean, this question about everything being anonymous, everything is not anonymous. At a minimum, we have got pseudo-anonymous logs. We have got one-way hashes. Those identifiers can be linked back by somebody to the IP address because we are updating the profiles. So it is just not that simple.

Senator DORGAN. One further point and then I will call on my colleague.

Mr. DYKES. Could I interject to say that clearly represents a misunderstanding of how we operate? And I will take time to talk to Ms. Harris some more.

Senator DORGAN. If we have time, we will come to that at the end.

One final point. This Committee did, on behalf of consumers, a Do-Not-Call List, obviously having to do with telephone solicitation. I am assuming that there are technical difficulties with a Do Not Track List. I have just described, when I started my questioning, why tracking with respect to my search for a book on a site really is probably beneficial to me, but I do not know what is being tracked of Senator DeMint's or my or Senator Carper's activities on the web. I do not have the foggiest idea who is tracking it, how they are tracking it, how they might use it, whether that company has some scruples and might be very careful about how it handles it or whether it is somebody else that grabs a hold of it and says, you know what, Katie, bar the door, I will sell it to anybody.

So that is the only question in my mind, that there are so many unanswered questions about information, how people navigate this web. The purpose of hearings, of course, is to try to inform and to understand, and that is the purpose of this hearing.

Let me call on Senator Carper who has not yet had an opportunity, and then I will call on Senator DeMint.

STATEMENT OF HON. THOMAS R. CARPER,
U.S. SENATOR FROM DELAWARE

Senator CARPER. I apologize for missing your presentations. As you know, we have a number of Subcommittees we serve on, and I have been detained at another hearing trying to figure out how to save the Medicare Trust Fund a couple hundred millions of dollars before it goes defunct.

And we are going to start voting I think in about 10 minutes.

Let me just use this as an opportunity to ask each of our witnesses to give me—maybe a minute apiece—a take-away. If we cannot remember everything you say—I would not pretend to. But each of you, give us a take-away. When we leave here, what would you have us keep in mind? Ms. Harris, why do we not start with you? Then we will just go to Mr. Kelly and Mr. Crews.

Ms. HARRIS. I mean, I think the key take-away is that we are in a very robust online environment where we get great benefit from the advertising, but we are collecting more and more information about consumers at the time that the information that consumers are putting online is increasingly personal and sensitive, health data, location data. Self-regulation is a piece, but self-regulation alone is not enough to protect privacy. And we need to have some baseline rules in place.

We have hearings and we bring in the companies who are good actors, who are at least willing to talk to privacy groups. It is a very big Internet, and we have to have some baseline for everybody.

Senator CARPER. And who should provide the baseline guidance? Should the industry police itself?

Ms. HARRIS. Well, I am saying self-regulation plays a key. It forces the boats up, but it is not in and of itself a solution and we

think that Congress has to pass a baseline privacy law. We have been advocating for years for that.

Senator CARPER. All right. Thank you.

Mr. Kelly?

Mr. KELLY. Facebook has been focused on transparency in the collection of information about what people do online. Senator Nelson offered an excellent example earlier. If he was reading an article—let us say it was in the *Miami Herald* online, the only way that Facebook would know that he is reading that article is if he hits the share button on his browser and it says, you know, share it with my Facebook friends. And at that point, the information would be collected. There is real-time notice. It would show up in his mini-feed of activity on the site and be presented to him.

And we are also committed to—if somebody wanted to target any advertising against that, if he wanted to become a fan of the *Miami Herald* on Facebook, that would be done in an anonymous space. The advertiser would not find out that Senator Nelson was a fan of the *Miami Herald.* They would just be able to target advertising toward fans of the *Miami Herald* on Facebook.

Senator CARPER. All right. Thank you.

Mr. Crews?

Mr. DYKES. So——

Senator CARPER. Go ahead, Mr. Dykes. You had a point on this?

Mr. DYKES. Yes. I was going to say NebuAd would welcome regulation in this area that was technology- and business process-neutral and focused on the privacy elements. Obviously, there should be strong controls, for more sensitive information and more personal information, including pseudo-anonymous information as Ms. Harris mentioned. I think that would be the criteria on which rules should be established. But room should be left for innovation because we just do not know how the Internet is going to evolve in the future, and so there is definitely a role for self-regulation by industry groups in this sphere as well.

Senator CARPER. Does anybody on our panel agree with anything that Mr. Dykes just said? I saw some nodding.

Ms. HARRIS. I came close.

[Laughter.]

Senator CARPER. I think, Mr. Crews, it is your turn.

Mr. CREWS. I was just going to mention that if the kind of profiling that we are all worried about here today is an inherent feature of the Internet, one of the things we have to worry about is what criminal elements are doing. In this debate, it is not just self-regulation or no regulation. There is a lot of competitive discipline that has to take place and will take place here.

But because of new technologies—as I said, it is only 2008. There are a lot more technologies that are going to come to fruition, including biometrics, including the face scanners and that data getting incorporated. There are a lot of institutions that have to evolve. I mean, markets do not pop into being, but the institutions that surround them to legitimize what industries do and to legitimize and establish a set of business practices that make sense that consumers live with have to evolve along with those new technologies. You do not want regulations that impede that.

I mean, take a look at the things that do work. Look at where opt-out is working. Look at where companies are already adopting opt-in procedures for certain kinds of information, and pay close attention to how important that is that those kinds of evolutions happen. Do not do something that thwarts them because there could be political failures just as there are market failures.

One of the inherent problems here too is that compulsory databases that Government mandates of all sorts can get blurred with private databases, and then that creates a problem. I call it the Social Security problem sometimes. You know, one of the trickiest personally identifiable indicators is the Social Security number. Well, here we are with an Internet that has come out. We cannot pull the rug out from under commerce and ban the use of the Social Security number, but we can move toward a future where business generates its own identifiers apart from that.

So those kinds of evolutions have to occur and we do not want to do specific regulations that might impede that because it is not a matter of self-regulation or no regulation. It is competitive discipline or——

Senator CARPER. Thank you.

Is it Mr. Hintze or Mr. Hintze?

Mr. HINTZE. Hintze.

Senator CARPER. Hintze. OK. I was wrong on both counts. Mr. Hintze.

Mr. HINTZE. I think there are a couple of take-aways from today.

One, we believe that protecting consumer privacy is not only compatible with the business of online advertising, it is essential to the success of the online advertising business. If consumers lose trust in this, if lawmakers are uncomfortable with how it is operating, the reaction could ultimately undermine this very important business model.

Microsoft itself has taken a number of concrete steps to protect consumer privacy that we think show our leadership in this space, but we are a relatively small player in the online advertising space. So we believe that also baseline privacy legislation is appropriate, supplemented by robust self-regulation, supplemented by technology tools, and supplemented by consumer education. They all need to work together to protect consumer privacy in the space.

Senator CARPER. Thank you.

And Ms. Horvath?

Ms. HORVATH. I would agree with what the other panelists have said. I guess our key take-away would be the need for a baseline Federal privacy statute which would be based upon the fair information practices that have been around for 20 years and would give consumers some feeling of accountability, that the companies have accountability to them for what they say they are doing with their information.

We would also support self-regulatory standards for the advertising sector. We also are already supportive of the NAI which has the first set of self-regulatory standards that are actually in effect right now.

Senator CARPER. Thank you.

Ms. Parnes, you are here, but I believe——

Senator DORGAN. Your time has expired.

Senator CARPER. OK, thank you very much.

Senator DORGAN. Senator DeMint?

Senator DEMINT. Thank you, Mr. Chairman. I know we are out of time.

A last comment. I spent all my career in advertising. So I know for many, many years we have been able to buy mailing lists that reflect behaviors. If someone subscribes to an outdoor magazine, you know they are likely to buy other things.

One of the exciting things about the Internet is, recognizing that most of the jobs in our country are created and maintained by small businesses, the Internet gives small companies the opportunity to invest advertising in a very targeted way. And the ability to use behavioral data to create market baskets that would allow smaller companies to focus their ad dollars on people who are most likely to buy their products is very, very important. And it is important that we maintain this. And I think it is very important that our Government look at creating laws and not try to manage the business, which is a very difficult line for us to draw.

My hope would be that the industry would recognize that consumers need to know what data about them is being collected and held, and that needs to be disclosed and very transparent so that the consumers become the regulators of the Internet. If they know, they will be able to switch to different content providers, different servers that are doing it better and better.

So my encouragement to the panel, those of you who are involved in the industry, is not to ask the Federal Government to come in at this point and to attempt to regulate because that is much different than a law that says how you can use data. I think as you continue to develop your technology, the disclosure and transparency to consumers is the best way to make sure that we end up with a vehicle that not only benefits consumers but is great for our economy.

So, again, Mr. Chairman, I thank you and I think this has been very eye-opening and enlightening. And I yield back.

Senator DORGAN. Senator DeMint, thank you very much.

Senator Carper, did you wish to ask additional questions?

Senator CARPER. On a lighter note, I have just come from a hearing where everyone spoke and testified to us using acronyms. And one guy used five acronyms in one sentence, and I had no idea what he said. I have no idea what he said.

[Laughter.]

Senator CARPER. I walk in here and people are talking about one-way hashes and cookies. I think the Chairman threw in something I think called the Flying Other Brothers. I am pretty good on music, but that is a new one to me. I was not here long, but it certainly has been illuminating. I obviously have to update my dictionary.

Thank you.

Senator DORGAN. Did you understand dementia and postnasal drip?

[Laughter.]

Senator CARPER. All too well.

[Laughter.]

Senator DORGAN. The Flying Other Brothers is actually a band that includes one of the Grateful Dead members, and they just have very bright tie-dyed T-shirts.

[Laughter.]

Senator DORGAN. Let me thank all of the witnesses for being here. I intend to have a hearing asking a number of the Internet service providers to come and visit with us. I think one of the most important elements coming from this hearing is how little we do understand. I think knowledge is important here. So I think most of us would like to understand what we can about what is happening, what kind of information is collected about our habits, about our movements, about our travels on the Internet. The Internet is really a wonderful thing. It brings the world to your fingertips.

Because I come from a town of 250 or 280 people, in my high school we had a coat closet-sized library. I mean, literally a coat closet that they turned into a library, just a few books. I do not need someone suggesting that is obvious.

[Laughter.]

Senator DORGAN. But I do think now in those little schools, the libraries are accessible by the Internet, the best libraries in the world. It really brings the world to our fingertips.

But there are legitimate questions raised about our traveling over the Internet and who watches us and how that information is used. I think we need to understand much more about it. There are those who raise questions about the use of information. I think those are very important questions. The reason that the Federal Trade Commission has developed a set of guidelines, self-regulatory guidelines, is because I think you understand the potential exists for abuse.

And I think the last thing that Senator DeMint described is something I certainly agree with. I would hope that every consumer has an opportunity, when traveling on the Internet, to understand what kind of information trail they leave and who might want to use that, or who is using it, or how is information about what is happening or what they are doing on the Internet going to be used. Information will give people an opportunity to decide, do they like the policies of this particular site or that particular provider, or do they wish to move elsewhere where policies are, they feel, more beneficial to their privacy.

So I think that this hearing has been instructive for us, and we will be announcing another hearing in which we will discuss this with the Internet service providers.

Senator CARPER. Mr. Chairman, would you yield for just a moment?

Senator DORGAN. Senator Carper?

Senator CARPER. In terms of the consumers being empowered to shop and to use the knowledge and understanding of these policies, probably every week we receive in our mail policy disclosures from a financial services company that we deal with. And my guess is that most of us do not take the time to look at it, and if we did, a lot of us would not understand it. So it is important if we are going to really enable the marketplace to work and to harness mar-

ket forces effectively, the information has to come in ways that consumers can actually internalize it, understand it, and find useful.

So thank you.

Senator DORGAN. I was just thinking that I frequently—and you perhaps do—get a letter in the mail from the North Dakota Drivers License Bureau saying someone made an inquiry about my driver's license and any potential infractions. I guess that is part of being in politics. Fortunately, it is clean and has nothing attached to the license. But that happens frequently. I assume there are a lot of people out there wondering about my driver's license. But at least we are notified. You are notified. I am notified when someone makes an inquiry and wishes to get that information.

And so that represents kind of the overhanging question here about who wants information, how do they use that information that represents personal information or other information about your travels on the Internet.

Let me thank the witnesses again. I appreciate your patience. And it works out that the vote, I believe, has just started.

This hearing is adjourned.

[Whereupon, at 11:48 a.m., the hearing was adjourned.]

A P P E N D I X

STATE OF CONNECTICUT
Hartford, CT, July 9, 2008

Hon. DANIEL K. INOUYE,
Chairman,

Hon. TED STEVENS,
Vice-Chairman,

Senate Committee on Commerce, Science, and Transportation,
Washington, DC.

Dear Senators Inouye and Stevens:

I appreciate the Senate Committee on Commerce, Science, and Transportation holding a hearing on the critically important issue of tracking consumer Internet use for marketing purposes. I urge expeditious Federal action to stop Internet service provider and third party marketer tracking of consumer Internet use for marketing purposes without prior and explicit consumer approval.

Monitoring consumer Internet browsing is a gross invasion of privacy for the sake of profit. It threatens to make every consumer's life an open book. Widely strewn to unknown websites and marketers would be highly sensitive and personal information such as medical conditions or family problems and financial interests.

In this brave new world, every movement or activity by consumers on the Internet will be recorded, collected and compiled into huge databases and then sold to marketers. Consumers will be bombarded with relentless and repeated advertising. Their personal activities and interests will be exposed to potential security breaches, just as countless breaches nationwide have opened private confidential financial information to potential misuse and identity theft.

This problem is neither speculative nor specious, It is very real and it is imminent. We are on the cusp of a new deep, enduring paradigm, fraught with perils to privacy.

Charter Communications, a cable and Internet service provider with customers in Connecticut and throughout the nation, recently announced a pilot program to give consumers "an enhanced Internet experience." These so-called enhanced services amounted to nothing more than spying on consumer web browsing by NebuAd. After I called on Charter to stop this initiative, it announced that it was canceling the pilot testing program. Charter has failed to disavow or deny future plans to track consumer Internet activities. Two phone companies—Embarq Corp. and CenturyTel—have completed trial tracking programs. Besides NebuAd, other tracking marketers are seeking targets of opportunity.

While Congress has sought to protect consumer privacy by enacting legislation such as the Cable Communications Policy Act, 47 U.S.C. 551 *et seq.*, and the Electronic Communications Privacy Act, 18 U.S.C. 2510 *et seq.,* both laws must be strengthened to emphatically and effectively ban tracking by Internet service providers and third party marketers. Congress should act promptly to address this new Internet menace.

I urge your quick and decisive action. I hope to be of assistance to the Committee in its work on this important initiative. Thank you.

Very truly yours,

RICHARD BLUMENTHAL,
Attorney General.

RESPONSE TO WRITTEN QUESTIONS SUBMITTED BY HON. MARIA CANTWELL TO LYDIA B. PARNES

Question 1. Ms. Parnes, do you believe consumers read online privacy policies?

Answer. Available research suggests that some consumers read online privacy policies, but many do not. Moreover, those that do read online privacy policies may

not do so consistently, and they typically do not review policies for changes after the initial read. For example, in a 2006 survey, only 20 percent of consumers said that they read the privacy policy when first providing information to a website "most of the time," although 43 percent said they had read an online privacy policy. Only 5 percent of consumers reported that they frequently check to see if privacy statements have been updated or revised.[1]

Although the reasons that consumers do not read online privacy policies may vary, we believe one key reason is that privacy policies are often too difficult to understand and/or too long. Research confirms this. For example, in a 2008 survey, the main reasons consumers reported for not reading privacy policies were because the polices contain too much legalese or jargon (57 percent) and that they take too long to read (58 percent).[2] Another study found that typical privacy policies require college-level reading skills to understand.[3] In addition, several studies show that significant numbers of consumers believe that the mere presence of a privacy policy on a website indicates some level of substantive privacy protection for their personal information.[4] As a result, once these consumers see that a privacy policy exists, they may believe it unnecessary to read the policy.[5]

The FTC staff recognized the concerns about online privacy policies when it issued its Proposed Self-Regulatory Principles. Because online behavioral advertising is largely invisible and unknown to consumers, the principles recommend that companies provide greater transparency about the practice through a "clear, concise, consumer-friendly and prominent" disclosure—that is, not through a disclosure cloaked in legalese and buried in a privacy policy. We are encouraging companies to develop creative ways to provide this disclosure, including by placing it outside of the privacy policy.

Question 2. Ms. Parnes, does the Commission view an End User Licensing Agreement as a contract between the online consumer and the website visited?

Answer. An "End User License Agreement," "Terms and Conditions" page, or similar document available on a website may be an enforceable contract between the online consumer and the website visited, depending on the particular circumstances and applicable state contract law. Courts have frequently held that when consumers click an "I Agree" icon in an online transaction (a.k.a., "clickwrap agreements"), and the terms and conditions to which they agree are readily available for review in advance via a hyperlink or in a scrollable window, those consumers are bound by those terms and conditions.[6] It is less clear whether courts would hold that an ordinary consumer would be bound by an agreement or other document where the consumer uses the website without actual knowledge of the terms and conditions posted there.[7]

However, in enforcing Section 5 of the FTC Act, it is generally unnecessary for the Commission to determine whether a EULA is, or is not, a contract. Under core FTC deception principles, disclosures buried in a EULA cannot be used to contradict a company's other representations, nor are they adequate to correct misimpressions

---

[1] *See* TRUSTe/TNS Survey (December 2006), available at *https://www.truste.org/about/press_release/12_06_06.php.*

[2] *See* AOL/DMS, "2008 AOL Consumer Survey on Behavioral Advertising" (February 2008).

[3] Irene Pollach, "What's Wrong with Online Privacy Policies?," Communications of the ACM, 50(9), 103–108 (2007).

[4] *See, e.g.,* 2007 Golden Bear Omnibus Survey (47.8 percent of consumers surveyed believe that, if a website has a privacy policy, it cannot share information with affiliate companies, and 55.4 percent believe that it could not sell information to other companies); Joseph Turow, Lauren Feldman, and Kimberly Meltzer, "Open to Exploitation: American Shoppers Online and Offline," Annenburg Public Policy Center, University of Pennsylvania (June 2000) (59 percent of consumers surveyed believe that a privacy policy on a website means that the site will not share consumer information with other websites or companies).

[5] *See, e.g.,* Joseph Turow and Chris Jay Hoofnagle, "The FTC and Consumer Privacy In the Coming Decade," at 17, presented at "Protecting Consumers in the Next Tech-Ade" (Nov. 8, 2006), available at *http://works.bepress.com/chris_hoofnagle/4/.*

[6] *See, e.g., Novak* v. *Overture Services, Inc.,* 309 F. Supp.2d 446, 450–51 (E.D.N.Y. 2004) (court holds that plaintiff, by clicking an "I accept" icon agreeing online to be bound by the "Terms of Service" governing use of an online discussion group set forth in a scrollable window, viewable ten lines at a time, was bound by the forum selection contained therein).

[7] *See, e.g., Specht* v. *Netscape Commc'ns Corp.,* 306 F.3d 17, 23–24, 35–38 (2d Cir. 2002) (refusing to enforce agreement against consumers); *see also Douglas* v. *Talk America Inc.,* 495 F.3d 1062, 1066 (9th Cir. 2007) (*per curiam*) (customer of long-distance service provider not bound by new contractual terms requiring arbitration of dispute when service provider merely posted them on its website and gave no notice to customer); *Waters* v. *Earthlink, Inc.,* 91 F.App'x 697, 698 (1st Cir. 2003) (refusing to enforce an arbitration clause posted on a website in the absence of proof the consumer had seen the clause).

that the company's representations would otherwise leave.[8] The Commission analyzes EULA-only disclosures on a case-by-case basis, weighing what information is material to consumers and the overall, net impression of the transaction.[9]

Question 3. Ms. Parnes, the FTC focuses on consumer harms. Can you give me a couple of examples of the types of potential consumer harms from online behavioral advertising? Does the Commission view a loss of any degree of personal privacy as being "a harm?"

Answer. The greatest risk of harm arises when information collected about a consumer's online activity is retained but not properly protected. Here, the Commission's work on data security informs our concern that information is sometimes retained beyond the point when it is needed, or without being well-protected. One possible harm from the collection of information for behavioral advertising is that it could be hacked or otherwise obtained and used for unauthorized purposes. Second, online behavioral advertising can lead to advertising and other communication with a consumer that reveals highly personal information and that can be unwelcome if it relates to sensitive issues, such as health or children, or is delivered in a shared computer environment. For example, in a situation where multiple users share the same computer, the delivery of behaviorally-targeted advertising might reveal the fact that a user conducted searches relating to AIDS, domestic abuse, or sexual preference.

As to whether a loss of personal privacy constitutes a "harm," it depends on the consumer. Different consumers may have different expectations about how their information is collected and used in this context, as well as different views about the information that they are willing to provide to obtain certain benefits—for example, coupons or free services. Indeed, in a survey conducted by Alan Westin,[10] 59 percent of the respondents were not comfortable with online tracking, yet 41 percent were "very" or "somewhat" comfortable." This is the main reason that Commission staff has proposed that companies provide consumers with choice concerning the collection of their data for the purpose of delivering behavioral advertising. Consumers who are comfortable with the practice can allow it, and consumers who are not comfortable can decline.

Question 4. Ms. Parnes, does the ability for advertisers to be able to link through a common field online, anonymous, behavioral marketing data and personally identifiable data typically used by marketers in the brick and mortar world provide any specific challenges to the Commission as it looks toward finalizing its principles on online behavioral advertising?

Answer. The ability to link non-personally identifiable information with personally identifiable information, and the debate concerning what online information is personally identifiable and what is not, have been among the central issues discussed in this area and in the comments to our proposed principles. Especially as technology advances, the line between the two categories of information becomes less and less clear. To the extent that non-personally identifiable information can become personally identifiable through reasonable technological efforts or linkages with other data, we believe it raises a concern. We are considering this issue carefully as we analyze the comments to our proposed principles and consider next steps.

Question 5. Ms. Parnes, I realize the Commission's principles on online behavioral advertising are just in a draft stage. In general, does the Commission have the authority to enforce any principle for self-regulation it may develop? If it does have this authority, how does the Commission intend to enforce the self regulatory principles on online behavioral advertising once they are finalized?

Answer. Several of the proposed self-regulatory principles reflect requirements of existing law and the Commission has made enforcing these principles a high pri-

---

[8] *See, e.g., Zango, Inc.,* FTC Docket No. C–4186 (2007) (complaint alleged that adware distributor represented that consumers could download free software and games and failed to disclose adequately that adware was bundled in the download; adware was often disclosed only in lengthy terms and conditions or through inconspicuous hyperlinks); *FTC* v. *Odysseus Marketing, Inc.,* No. 1:05–CV–00330–SM (D. N.H. 2006) (complaint alleged that defendants deceptively failed to disclose adequately that their software would collect consumers' personal information and substantially alter behavior of computers where those functions were disclosed only in EULA accessible via inconspicuous hyperlink).

[9] *See Sony BMG Music Entertainment,* FTC Docket No. C–4195, Letter responding to comment from Jerry Berman, Center for Democracy and Technology (June 28, 2007); *Zango, Inc.,* FTC Docket No. C–4186, Letter responding to comment from Mark Bohannon, Software & Information Industry Ass'n (Mar. 7, 2007).

[10] *See* Alan Westin, "How Online Users Feel About Behavioral Marketing and How Adoption of Privacy and Security Policies Could Affect Their Feelings," at 3 (March 2008).

ority. The agency will continue to enforce laws within our jurisdiction as necessary to protect consumers. For example, the principles maintain that companies should provide reasonable security for behavioral data so that it does not fall into the wrong hands. The Commission has brought numerous enforcement actions focusing on the obligation of companies that collect or store consumer data to provide reasonable security for that data.[11] In addition, the principles provide that before a company uses behavioral data in a manner that is materially different from promises made when the data was collected, it should obtain affirmative express consent from the consumer. The Commission has brought high-profile law enforcement actions against companies that violated this principle by using data in a manner materially different from promises the company made at the time of collection.[12] In addition, if a company made material misrepresentations about the collection or use of behavioral advertising data, such misrepresentations would constitute a deceptive practice, in violation of Section 5 of the FTC Act.

The purpose of the FTC staff's proposed principles is to encourage more meaningful and enforceable self-regulation. Because strong enforcement mechanisms are necessary to ensure effective self-regulation, it is our expectation that the organizations developing self-regulation will include in their regimes mechanisms for meaningful enforcement.

Question 6. Ms. Parnes, as you know, in recent months, there have been deals announced between online search engines with strong online advertising market shares. Considering the implications these proposals have for market consolidation, is the Commission worried about the prospect of the vast majority of behavioral online information being in the hands of one company?

Answer. Market consolidation that results in the creation of vaster, more detailed databases of online consumer data may raise concerns. Although companies with large stores of data can be just as privacy-protective as those with small ones, the risks associated with data collection and storage, such as the risk that data could fall into the wrong hands, may be heightened where one company maintains large quantities of rich data. Further, competition ensures that companies have incentives to protect customer privacy, and market consolidation could undermine competition in this area.

However, whether there is cause for concern must be evaluated on a case-by-case basis. A given deal between online advertising companies may not involve the transfer or sharing of any data, or may not result in a more detailed database of consumer information than those already possessed by other companies in the online marketplace. The Commission can evaluate whether a proposed transaction would adversely affect non-price attributes of competition, such as consumer privacy, and will continue to do so as appropriate.

RESPONSE TO WRITTEN QUESTIONS SUBMITTED BY HON. DAVID VITTER TO LYDIA B. PARNES

Question 1. Do you believe legislation mandating the FTC's pending self-regulatory principles is necessary at this time?

---

[11] Since 2001, the Commission has obtained twenty consent orders against companies that allegedly failed to provide reasonable protections for sensitive consumer information. *See In the Matter of The TJX Companies,* FTC File No. 072–3055 (Mar. 27, 2008, settlement accepted for public comment); *In the Matter of Reed Elsevier Inc. and Seisint Inc.,* FTC File No. 052–3094 (Mar. 27, 2008, settlement accepted for public comment); *United States* v. *ValueClick Inc.,* No. CV08–01711 (C.D. Cal. Mar. 13, 2008); *In the Matter of Goal Financial, LLC,* FTC Docket No. C–4216 (April 15, 2008); *In the Matter of Life is Good, Inc.,* FTC Docket No. C–4218 (Apr. 18, 2008); *United States* v. *American United Mortgage,* No. CV07C 7064, (N.D. Ill. Dec. 18, 2007); *In the Matter of Guidance Software, Inc.,* FTC Docket No. C–4187 (Apr. 3, 2007); *In the Matter of CardSystems Solutions, Inc.,* FTC Docket No. C–4168 (Sept. 5, 2006); *In the Matter of Nations Title Agency, Inc.,* FTC Docket No. C–4161 (June 19, 2006); *In the Matter of DSW, Inc.,* FTC Docket No. C–4157 (Mar. 7, 2006); *United States* v. *ChoicePoint, Inc.,* No: 106–CV–0198 (N.D. Ga. Feb. 15, 2006); *In the Matter of Superior Mortgage Corp.,* FTC Docket No. C–4153 (Dec. 14, 2005); *In the Matter of BJ's Wholesale Club, Inc.,* FTC Docket No. C–4148 (Sept. 20, 2005); *In the Matter of Nationwide Mortgage Group, Inc.,* FTC Docket No. 9319 (Apr. 12, 2005); *In the Matter of Petco Animal Supplies, Inc.,* FTC Docket No. C–4133 (Mar. 4, 2005); *In the Matter of Sunbelt Lending Services,* FTC Docket No. C–4129 (Jan. 3, 2005); *In the Matter of MTS Inc., d/b/a Tower Records/Books/Video,* FTC Docket No. C–4110 (May 28, 2004); *In the Matter of Guess?, Inc.,* FTC Docket No. C–4091 (July 30, 2003); *In the Matter of Microsoft Corp.,* FTC Docket No. C–4069 (Dec. 20, 2002); *In the Matter of Eli Lilly & Co.,* FTC Docket No. C–4047 (May 8, 2002).

[12] *See, e.g., Gateway Learning Corp.,* Docket No. C–4120 (Sept. 10, 2004), *http://www.ftc.gov/opa/2004/07/gateway.shtm.*

Answer. I do not believe that legislation regarding online behavioral advertising is necessary at this time. As stated in the written testimony presented to the Committee on July 9, 2008,[1] the Commission is cautiously optimistic that the privacy issues raised by online behavioral advertising can be addressed effectively through self-regulation.

The online marketplace is undergoing rapid change. Many different types of businesses are entering the advertising market and the technologies utilized by these businesses are constantly evolving. At the same time, the costs and benefits of various types of behavioral advertising may be difficult to weigh. Although online behavioral advertising raises legitimate privacy concerns, it may provide benefits to consumers in the form of more personalized and relevant advertisements, as well as the free content that Internet users have come to expect. In this environment, industry self-regulation, which may afford the flexibility needed as online business models and technologies evolve, may be the preferred approach. Although there is much work to be done in this area, I believe that the self-regulatory processes that have been initiated by the Network Advertising Initiative (NAI) and other organizations should be given an opportunity to develop.

Question 2. Do you believe the same principles about transparency and choice would be necessary for behavioral advertising based on "anonymous" or non-personally-identifiable information?

Answer. The FTC received considerable comment on this issue in response to the staff's proposed self-regulatory principles. Many commenters stated, for example, that the collection of data that is not personally identifiable is unlikely to cause consumer harm and therefore should not be subject to the notice and choice requirements in the staffs proposed principles. Other commenters stated that, even when information collected is not personally identifiable, its use can lead to advertising or other contacts with a consumer that can be unwelcome or embarrassing, especially if they relate to sensitive issues, such as health, children, or a consumer's finances, or are delivered in a shared computer environment.

The comments also highlight the considerable debate that remains concerning what online information is personally identifiable and what is not, and the effect that advances in technology may have on the distinction. Further, incidents such as the AOL breach demonstrate that items of information that are considered anonymous standing alone may become personally identifiable when combined, challenging traditional notions about what data is or is not personally identifiable.[2]

FTC staff continues to carefully review the comments received on this issue, and we intend to address it as we develop our next steps in this area.

Question 3. Based on your experience, how is online behavioral advertising different from offline direct marketing? Also, what would be the justification for regulating online advertising differently than offline advertising?

Answer. Targeted marketing also exists in the offline environment. However, rapidly evolving Internet technologies permit online marketing companies to collect, store, and analyze significantly greater amounts of data than offline companies, and to do so through practices that are often invisible to consumers. Offline marketing generally involves the collection of a smaller quantity of less detailed behavioral information than is gathered online, and that collection is likely to be more consistent with consumer expectations.

For example, brick-and-mortar stores often record a consumer's purchase history and use it to market to the consumer. They typically do not, however, follow individual consumers around their stores and collect detailed information about the other products the consumer might have looked at, nor do they share purchase or behavioral information with third parties. Similarly, consumers know that subscribing to a newspaper involves the sharing of personal information so that the newspaper can be delivered to their homes; however, they generally would not expect every article read in a newspaper to be tracked and recorded by multiple parties. Given the amount and type of data that is collected and stored in connection with online behavioral advertising, and the invisibility and typically unexpected nature of such practices, it may be appropriate to take different approaches to protecting consumer privacy between online behavioral advertising and offline marketing.

---

[1] *See Privacy Implications of Online Advertising: Hearing Before the S. Comm. on Commerce, Science, and Transportation,* 110th Cong. (2008) (statement of the Federal Trade Commission), at 14.

[2] Although AOL took steps to anonymize the search records of its subscribers that were made public in 2006, several newspapers and consumer groups were able, to identify some individual AOL users and their queries by combining the data.

Question 4. Based on your experience, has the FTC identified any specific harm to consumers that has resulted from the information used for online behavioral targeting?

Answer. At this time, the FTC is unaware of any specific incidents in which a company's online behavioral advertising practices have led to such consumer harms as identity theft, financial fraud, or physical harm. Behavioral advertising, however, does raise unique concerns because of the amount, richness, and sensitivity of the consumer information that may be collected, used, and shared with third parties. For example, in a situation where multiple users share the same computer, the delivery of behaviorally-targeted advertising might reveal the fact that a user conducted searches relating to highly personal and sensitive topics, such as AIDS, domestic abuse, or sexual orientation. To the extent that the information collected is or could later become personally identifiable, the risk of harm may be greater.

Many consumers express concern about the privacy and data security implications of behavioral tracking. For example, a 2008 survey showed that 59 percent of those surveyed are "not very comfortable" (34 percent) or "not comfortable at all" (25 percent) with websites using online activity data to tailor advertisements or content to their hobbies and interests, whereas 41 percent were "comfortable" or "somewhat comfortable."[3] As this survey indicates, consumers differ in their level of concern about this practice and in how they weigh the benefits of more relevant ads against the privacy implications. For this reason, the Commission staff's proposed principles would require that companies provide consumers with choice concerning the collection of their data for the purpose of delivering behavioral advertising.

RESPONSE TO WRITTEN QUESTIONS SUBMITTED BY HON. MARIA CANTWELL TO CHRIS KELLY

Question 1. Mr. Kelly, as you mentioned in your written statement, Facebook's privacy policy states clearly that you believe all of your users "should have control over [their] personal information." However, as I understand it from my staff, many of whom have Facebook accounts, when members of Facebook wish to terminate the service, they are only allowed to "deactivate." Do you currently offer your members an opportunity to control their personal information by completely terminating their account and allowing Facebook to then delete their personal information? If not, why hold onto their information?

Answer. At Facebook, we reflect our desire to give users control over their information by providing them two options if they wish to suspend or terminate their relationship with us.

Facebook users can make either a temporary or permanent decision to shut down their account—the former is called deactivation, and the latter deletion. Users choose to deactivate their accounts for a variety of reasons. Given Facebook's roots as a college site, one original driver for introducing the deactivation feature was user desire to "disappear" during their exams and then resume the service with their friend connections and network membership intact. More than 50 percent of the users who deactivate their Facebook accounts return to reactivate them within weeks.

Deletion is a fuller option that erases the personally identifiable information such as name, e-mail address, IM handle and other core information from a Facebook account. While we cannot certify that every single piece of data a user has ever given us is irretrievable after the deletion process is done—the distributed nature of databases and Internet site operations, especially for a longstanding user, makes that certification practically impossible—we have scrubbed our active databases of all contact information for a particular account. A deleted account cannot be reconstructed; a user who wants to come back to use the Facebook service after undergoing the deletion process must start over with regard to setting up their friends and networks. I am unaware of a similar deletion option offered by any other major Internet company.

Question 2. Mr. Kelly, according to a *Washington Post* article from last month, Facebook requires 95 percent of its members that use one of the social network's 24,000 applications to give the applications' developers access to their personal online profile, except contact information, and their friends' profiles as well. While I understand these developers are not allowed to share with advertisers, this still leaves the 400,000 developers with access to personal information that is out of Facebook's control. A recent study at the University of Virginia found that about

[3] *See* Alan Westin, "How Online Users Feel About Behavioral Marketing and How Adoption of Privacy and Security Policies Could Affect Their Feelings," at 3 (March 2008).

90 percent of the most popular Facebook applications have unnecessary access to private data. So my question is, why does a Sudoku puzzle have to know that someone has two kids? And why does a book-sharing program need to know my birthday?

Answer. Facebook's developer terms of use do not just forbid sharing with advertisers of the information that applications request. They only allow retention of most data called from the Facebook service for 24 hours in order to facilitate the more rapid operation of the application. Retention for a period beyond that is forbidden. Requests for data through the Facebook API are logged, and the platform policy enforcement team conducts investigations as necessary to discover potential violations. They then take action up to and including barring an application or a developer from further use of the service where violations are discovered.

Users of course may choose to establish a deeper relationship with an application by providing more personal information directly, but Facebook's terms and policies work together to encourage strongly clarity with users about access to their data.

In addition to the technical and policy enforcement measures outlined here, Facebook is always looking for means to enhance transparency to users with regard to data collection and use. We are currently exploring efficient and effective means to give users greater knowledge of and control over data requests by applications so that a user will know if an application is seeking more data than the user believes is necessary. At that point, the user could then choose to remove the application from their profile, or to use the "block" feature that has been present since the introduction of the Facebook platform in 2007 that prevents any data from flowing to that application.

RESPONSE TO WRITTEN QUESTIONS SUBMITTED BY HON. DAVID VITTER TO CHRIS KELLY

Question 1. Does your company's business model already accommodate the FTC's proposed principles for industry self-regulation? If so, please explain how.

Answer. In putting in place baseline privacy controls that users can adjust to their liking and allowing users to make their own choices about the sharing of personal information with advertisers, we generally reflect the FTC self-regulatory principles. Our commentary on the principles has suggested that the FTC offer greater clarity in distinguishing between how personally and non-personally identifiable information should be addressed by the principles, which we believe will lead to greater consumer understanding and confidence.

Question 2. Does your system accommodate for a consumer's choice not to receive behavioral advertising, and in your systems, is that request honored permanently? If so, please explain how.

Answer. While Facebook does not currently engage in many of the behavioral targeting practices that have been the main focus of the Committee's attention, it bears noting at the outset that Facebook is an opt-in system at its core. If a user does not sign up for and use Facebook, they will not receive advertising through our service.

In addition to this fundamental user choice, we offer opt-outs for many of our advertising products within the Facebook ecosystem. For instance, those users who do not wish to participate in our Social Ads product have an easily available option to turn it off.

User control is a critical part of Facebook's philosophy and our offerings in the product and advertising area will continue to reflect that principle.

RESPONSE TO WRITTEN QUESTIONS SUBMITTED BY HON. MARIA CANTWELL TO JANE HORVATH

Question 1. Ms. Horvath, just a few months ago, in Google's comments to the FTC on self-regulatory principles for online advertising, the company said that "contextual advertising . . . is not the type of advertising that ought to be the focus of the FTC's efforts to develop effective self regulatory principles." I understand that contextual advertising is less invasive than behavioral advertising. However, I am interested to hear the rationale behind Google's belief that it should be exempt from the FTC's self-regulatory principle.

Answer. Google has not suggested that it or any other online advertiser be exempted from self-regulation with respect to behavioral advertising. We have said and continue to believe that further thought must be given to the definition of behavioral advertising in the Federal Trade Commission staff's draft self-regulatory principles. As currently written, the draft principles define "behavioral advertising"

so broadly as to encompass virtually any collection and use of information about a user's online activities, including the collection and use of information to provide contextual advertising.

AOL, Google, Microsoft, Yahoo!, and many other companies provide contextual advertising solutions, which, as you point out, are different from behaviorally targeted ads because they provide relevant advertising based on what an Internet user is searching for as well as relevant ads based on a page that a user is viewing. Though it is not the focus of our business today, Google believes that behavioral advertising can be done in ways that are responsible and protective of consumer privacy and the security of consumers' information.

To ensure the continuation and proliferation of responsible behavioral advertising practices, we are supportive of efforts to establish strong self-regulatory principles for online advertising that involves the collection of user data for the purpose of creating behavioral and demographic profiles. For example, we believe that the FTC's efforts to address this type of advertising through self-regulatory principles are appropriate and helpful. Likewise, we support the Network Advertising Initiative's recently-announced draft Self-Regulatory Code of Conduct for Online Behavioral Advertising, which includes limitation on the use of sensitive information to create profiles of individuals for purposes of third-party advertising.

For both the FTC's draft principles and the NAI's draft code of conduct, we believe that the focus on data collected across multiple web domains owned or operated by different entities to categorize likely consumer interest segments for use in online advertising is appropriate. We also believe that a strong and easy-to-find mechanism to permit consumers to opt out of this type of data collection is a goal that all companies should aspire to achieve. Finally, we believe that special attention should be given to rules around the creation of profiles based on sensitive information such as health status.

Question 2. Ms. Horvath, one of the central issues in the Internet privacy debate is the protection, or lack thereof, of personally identifiable information. I'm interested to know, what measures Google is taking to ensure that the data it uses for ad targeting is not connected to personally identifiable information? What opt-out mechanisms do you currently offer your customers? How robust are these opt-out mechanisms and how easy are these mechanisms for consumers to use?

Answer. Google protects its users' personally identifiable information—PII—in many ways. For example, we do not use PII to serve ads in connection with our AdWords and AdSense products. We also have strict policies and procedures in place to ensure that personal information is used only in accordance with our privacy policy, which is located at *www.google.com/privacy.html,* and that our users' personal information is secure.

We collect non-PII through the DoubleClick cookie in order to enable enhanced functionality to advertisers that use DoubleClick and advertisers that advertise on the Google content network through our AdSense for Publishers product. For example, this data collection will enable advertisers that advertise through AdSense for Publishers to limit the number of times a user sees an ad through frequency capping. Users will have a better experience on Google content network sites because they will no longer see the same ad over and over again.

Users are able to opt out of data collection through our DoubleClick ad serving cookie in several ways. For example, users can opt out by visiting the DoubleClick opt out page located at *www.doubleclick.com/privacy.* In addition, our ads privacy microsite has an above-the-fold opt out button located at *www.google.com/privacy_ads.html.* Users are also able to opt out of the DoubleClick cookie's data collection through the Network Advertising Initiative's opt out page located at *www.networkadvertising.org/managing/opt_out.asp.* This single opt-out is honored both in the DoubleClick network and in the Google content network.

Question 3. Ms. Horvath, in your written testimony, you indicate Google is currently experimenting to deliver search results based on prior searches. Isn't this behavioral advertising by any other name? Is this consistent with Google's privacy policy regarding behavioral advertising?

Answer. We are currently experimenting with providing ads on Google search based on both a user's current query and his or her recent prior queries. For example, a user who types "Italy vacation" into the Google search box might see ads about Tuscany or affordable flights to Rome. If the user were to subsequently search for "weather," we might assume that there is a link between "Italy vacation" and "weather" and deliver ads regarding local weather conditions in Italy. In the above example, we are serving an ad based on a user's activity on our site, and not the sites of other parties. This is an example of the kind of first-party advertising that users expect to see in response to the search terms they enter into the Google search

box. While we may use recent queries to better respond to the user's specific interests, this is done on the fly, and we are not building profiles based on a users' search activities.

Google's privacy policy, which is located at *www.google.com/privacy.html,* states clearly that we use this information to provide our services to users, including the display of customized content and advertising. We also provide plain English explanation of our advertising and privacy practices on our ads privacy microsite located at *www.google.com/privacy_ads.html.*

Question 4. Ms. Horvath, with regard to Google's recently announced marketing deal with Yahoo!, are you able to tell us what information Yahoo! will share with Google? Will it include IP addresses? If so, has Google done its due diligence to ensure that the transfer of data from Yahoo won't violate Yahoo!'s privacy policy? As you know, Yahoo! has publicly announced it will retain information about consumer search queries for 13 months. I believe your company retains such information for 18 months. Does Google intend to conform to Yahoo!'s retention policy or is Yahoo! expected to conform to Google's?

Answer. Under our advertising agreement with Yahoo!, there is no PII passed between Yahoo! and Google. In fact, for ads appearing (impressions) on Yahoo! Search, Yahoo! will remove the last octet of the IP address before sending us search queries, so Yahoo will never send the full IP address to Google. Moreover, in the search advertising context Google will set a cookie only if a user clicks on an ad delivered by Google.

RESPONSE TO WRITTEN QUESTIONS SUBMITTED BY HON. DAVID VITTER TO JANE HORVATH

Question 1. Does your company's business model already accommodate the FTC's proposed principles for industry self-regulation? If so, please explain how.

Answer. We have participated actively in the Federal Trade Commission's efforts to develop privacy principles relating to online privacy and behavioral advertising. Our hope is that the FTC's privacy principles—once finalized and written to ensure that they can be realized by industry and will provide consumers with appropriate levels of transparency, choice, and security—will be adopted widely by the online advertising industry and will serve as a model for industry self-regulation in jurisdictions beyond the United States.

Our comments on the FTC's principles are available at *googlepublicpolicy.blogspot.com/2008/04/our-comments-on-ftcs-behavioral.html.* In addition, through DoubleClick we are members of and serve on the Board of Directors of the Network Advertising Initiative and abide by the NAI Self-Regulatory Principles.

Question 2. Does your system accommodate for a consumer's choice not to receive behavioral advertising, and in your systems, is that request honored permanently? If so, please explain how.

Answer. Though our business is focused on contextual advertising, we collect non-personally identifiable information through our DoubleClick ad serving cookie in order to enable enhanced functionality to advertisers that use DoubleClick and advertisers that advertise on the Google content network through our AdSense for Publishers product. For example, this data collection will enable advertisers that advertise through AdSense for Publishers to limit the number of times a user sees an ad through frequency capping. Users will have a better experience on Google content network sites because they will no longer see the same ad over and over again.

Users are able to opt out of data collection through our DoubleClick ad serving cookie in several ways. For example, users can opt out by visiting the DoubleClick opt out page located at *www.doubleclick.com/privacy.* In addition, our ads privacy microsite has an above-the-fold opt out button located at *www.google.com/privacy_ads.html.* Users are also able to opt out of the DoubleClick cookie's data collection through the Network Advertising Initiative's opt out page located at *www.networkadvertising.org/managing/opt_out.asp.* This single opt-out is honored both in the DoubleClick network and in the Google content network.

We believe that a strong and easy-to-find mechanism to permit consumers to opt out of this type of data collection is a goal that all companies should aspire to achieve.

RESPONSE TO WRITTEN QUESTIONS SUBMITTED BY HON. MARIA CANTWELL TO LESLIE HARRIS

Question 1. Ms. Harris, do you believe consumers read online privacy policies?

Answer. There is ample evidence that consumers do not read privacy policies and to the extent that they do, they do not understand them. Indeed, a recent study found that over half of respondents believed that the presence of a privacy policy on a website meant that the site did not share or sell personal information. Moreover, privacy policies often are in practice disclosure policies, making no promises to protect customer information and instead stating all the ways the site intends to use and disclose data. Consumers need clear, conspicuous and understandable notice of collection and disclosure practices.

Question 2. Ms. Harris, do you view an End User Licensing Agreement as a contract between the online consumer and the website visited?

Answer. End User Licensing Agreements are typically included when consumers purchase or download software. Courts generally have held that these EULAs do constitute contracts between consumers and the companies distributing the software, though it may depend on factors such as the prominence of the EULA and whether consumers affirmatively express agreement (by clicking an "I Agree" button, for example). As a practical matter, as we have seen in the case of malicious "spyware" and as the FTC has recognized in its settlement agreements with spyware purveyors, long, complicated EULAs are wholly inadequate to inform consumers about the material effects that a particular piece of software will have on their computers. The FTC has set the right precedent in requiring simple explanations of such key information outside of any software EULA. Outside the software context, it is less clear that merely visiting a website would be sufficient to contractually bind a consumer to a Terms of Service agreement, particularly in the absence of some express indication of consumer acceptance. The FTC has made, clear, however, that websites must adhere to their publicly stated policies on matters such as privacy, or risk possible charges of deception.

Question 3. Ms. Harris, as you know the FTC focuses on consumer harms. Do you believe that some of the issues surrounding online behavioral advertising go beyond what the Commission has traditional viewed as consumer harm?

Answer. The FTC has traditionally focused on tangible harms such as practices which result in a financial loss or which induce a consumer to engage in a transaction through deceptive practices. We do not believe that the privacy concerns raised by behavioral advertising are limited to those which result in an adverse action against a consumer. The right of privacy is harmed when consumers have no reasonable expectation that information about them is being collected, they are not provided meaningful notice that would allow them to gauge the privacy risks, and they have no way to make meaningful decisions about whether and how their information may be used.

Question 4. Ms. Harris, should online contextual advertising be exempt from any self regulatory framework or does the Commission only need to look at behavioral advertising?

Answer. Contextual advertising, which is often used to generate ads alongside search results, matches advertisements to the content of the page that a consumer is currently viewing. The privacy risks associated with contextual advertising vary. If the practice is transparent to the user and data collection and retention is minimal, the practice poses little risk to the consumer. For example, if a site only looks at the consumer's activity and only serves ads based on that activity contemporaneously , *i.e.,* at the moment the consumer is engaging in the activity and does not collect and save the consumer data, the privacy concern is low. But the privacy concerns are heightened if the user data is retained in an identifiable or pseudonymous form (*i.e.,* linked to a user identifier) for long periods of time even if it is not immediately used to create advertising profiles.

CDT has long advocated for a baseline privacy bill that would cover all collection and use of consumer data and require the full range of fair information practices, which include but are not limited to robust notice and consumer choice but also provide penalties for noncompliance and remedies for consumers. Self regulation is not enough. To the extent that self-regulation remains as one component of privacy protection in this area, consumers will certainly benefit from a self-regulatory scheme that covers both contextual and behavioral advertising, with escalating protections for models with increased data collection, retention, use, and identifiability.

Question 5. Ms. Harris, are you concerned with the recently announced marketing deal between Google and Yahoo! that one company will have under its control the vast majority of consumers' online behavioral information?

Answer. The Google/Yahoo! marketing deal does have the potential to consolidate more data about search and search advertising under one roof. While this data is certainly one component of behavioral information, Google does not currently use search data to create behavioral profiles. Thus, the more relevant question is whether the consolidation of search information—not necessarily behavioral information—is of concern.

This deal follows in the footsteps of a series of major mergers and acquisitions in the online advertising space over the past 18 months. All of this market consolidation means that more and more data about what consumers do online is housed by fewer companies, exacerbating existing privacy concerns about how such data is collected, used, safeguarded, and shared. We believe that recent market dynamics are even further evidence of the need for a general privacy law to protect consumer data at large.

QUESTION FOR THE RECORD FROM HON. DAVID VITTER TO LESLIE HARRIS

Question. As our committee continues to examine the issue of online privacy, should we focus on the variations in different technologies used to provide what appears to be essentially similar marketing services? Or, should we instead focus on the use of the information collected—by whatever method it is collected—to ensure that data is used for legitimate marketing purposes, that privacy is protected, and that we can go after those who misuse any data they collect?

[The witness did not respond.]

RESPONSE TO WRITTEN QUESTIONS SUBMITTED BY HON. MARIA CANTWELL TO ROBERT R. DYKES

Question 1. Mr. Dykes, over the last few weeks numerous Internet service providers, including CenturyTel, Charter and Wide Open West have either ceased using your service or shelved any plans they had to do so. What does this tell you about your proposed business model and consumer reaction to it?

Answer. NebuAd and its Internet service provider ("ISP") partners have always been and continue to be committed to the core privacy principles of transparency and consumer control regarding NebuAd's services. We support our ISP partners' decisions to delay their implementation plans so they can ensure that in deploying NebuAd's services, customers receive clear, direct, and prior notice that NebuAd's services will take effect, thereby allowing subscribers to make an informed choice regarding whether to participate.

NebuAd plans to continue to explain our existing business model and better educate the public about the state-of-the-art privacy protections that have been built-in to NebuAd's services, and, equally as important, the process that we have established to continuously improve on them. In support of this process to continuously advance privacy protections beyond industry standards, NebuAd looks forward to a continued open dialogue with legislators, regulators, and the advocacy community.

NebuAd remains committed to delivering strong value to advertisers, publishers, and ISPs while setting the gold standard for privacy in online advertising and delivering the best Internet experience possible to consumers.

Question la. Do you believe that consumers have the perception that your technology will allow ISPs to watch over every move they make on the Internet?

Answer. A close examination of NebuAd's technology, operations, and privacy protections demonstrates that it is a responsible, privacy conscious business. Unfortunately, some recent public statements from various sources have presented inaccuracies, distortions, and misrepresentations of our technology and business model. While some consumers may have formed mistaken perceptions based on these erroneous statements about the NebuAd technology, the privacy controls in place, and the business model in conjunction with our ISP partners, we believe that consumer education is a key component of our continued effort to set the gold standard for privacy in online advertising.

Finally, as a point of clarification, NebuAd does not watch every move consumers make on the Internet. The NebuAd system only uses a select set of a consumer's Internet activities (that is, only a subset of HTTP traffic) to construct anonymous inferences about the consumer's level of qualification for a predefined set of market segment categories, which are then used to select and serve the most relevant advertisements to that consumer. The NebuAd system does not collect or use any information from password-protected sites (*e.g.,* HTTPS traffic), web mail, e-mail, in-

stant messages, or VoIP traffic, and the system does not make use of any market segments that are deemed to be sensitive.

Question 2. Mr. Dykes, in your written testimony you praise online advertising, especially NebuAd's approach, for enhancing consumers' Internet experience. As you know, the most important quality to Internet users is the speed of their Internet connection. How does the NebuAd's approach to behavioral monitoring—deep packet inspection—affect the speed of a consumer's connection, including uploads and downloads?

Answer. NebuAd's service does not adversely affect either upload or download performance. The NebuAd Ultra Transparent Appliance ("UTA") is *transparent* when it comes to performance impact. Lab-tests of the NebuAd UTA and have found the performance of the NebuAd UTA matched or exceeded standard performance metrics expected from any network device such as a switch and/or a router. In addition, NebuAd has sophisticated monitoring capabilities to ensure performance expectations are maintained.

RESPONSE TO WRITTEN QUESTIONS SUBMITTED BY HON. DAVID VITTER TO ROBERT R. DYKES

Question 1. Does your company's business model already accommodate the FTC's proposed principles for industry self-regulation? If so, please explain how.

Answer. NebuAd participated in the FTC's proceeding by submitting written comments on the proposed principles. A copy of NebuAd's comments is available at *http://www.ftc.gov/os/comments/behavioraladprinciples/080411nebuad.pdf* ("NebuAd Comments"). In its written comments, NebuAd agreed with the FTC Staff that the "self-regulatory principles that emerge from this process must rest within an overall framework that promotes transparency, consumer control, limited use of sensitive information, limited data storage, and strong security."

NebuAd's comments focused on a central theme: any set of final proposals for self-regulation should focus on the ultimate goal—preventing consumer harm—and not on regulating different behavioral advertising technologies and companies in different ways based simply on the underlying technology used or individual entities involved. In other words, NebuAd believes that the final self-regulatory principles that emerge from the FTC proceeding must be consistent with the twin objectives of technology-neutrality and provider and publisher-neutrality. This will allow for innovation within a flexible self-regulatory framework while preventing an unintended consequence of inadvertently picking winners and losers in the emerging behavioral advertising marketplace, based solely on technology or business model.

NebuAd looks forward to the Commission Staff's release of its final principles. Like the Federal Trade Commission, NebuAd is "cautiously optimistic" that industry self-regulation will work to protect consumers. *See* Prepared Statement of the Federal Trade Commission on Behavioral Advertising, Before the Senate Committee on Commerce, Science, and Transportation (July 9, 2008) at 1, available at *http://www.ftc.gov/os/2008/07/P085400behavioralad.pdf*. Moreover, NebuAd has joined a chorus of other companies in calling for baseline privacy legislation. See oral testimony of Mr. Robert R. Dykes, Chairman and CEO, NebuAd, Inc, in hearing before the Subcommittee on Telecommunications and the Internet: *What Your Broadband Provider Knows About Your Web Use: Deep Packet Inspection and Communications Laws and Policies,* July 17, 2008.

NebuAd's specific response to this question is as follows. (The FTC's Proposed Principles for the Self-Regulation of Behavioral Advertising are available at *http://www.ftc.gov/os/2007/12/P859900stmt.pdf*).

Principle 1: To address the need for greater transparency and consumer control regarding privacy issues raised by behavioral advertising, the FTC staff proposes:

- Every website where data is collected for behavioral advertising should provide a clear, consumer-friendly, and prominent statement that data is being collected to provide ads targeted to the consumer and give consumers the ability to choose whether or not to have their information collected for such purpose.

NebuAd Response: NebuAd supports the underlying goal of this proposal, which is to ensure that consumers are provided with ample opportunity to understand what information is collected, by whom, for what purpose, and to provide consumers with control over their online experience. Unfortunately, the proposal, as written, is problematic for NebuAd for reasons that are business-model specific, and having nothing to do with providing consumers with meaningful transparency and consumer control. As we noted in our comments to the FTC,

"[t]his proposal is apparently addressed to behavioral advertising companies that, unlike NebuAd, have direct relationships with those websites, typically as part of a network. Because NebuAd works through ISPs and other ad networks and does not necessarily have direct relationships with the websites consumers visit, it has no way to require them to post the proposed notice. For this reason, NebuAd respectfully asks the Commission Staff to consider alternative methods of notice, such as direct notice provided by ISPs to their subscribers, together with an opportunity to opt-out, as an appropriate means of meeting the Staff's proposed transparency principle."

See NebuAd comments at p. 4. In other words, NebuAd is in full agreement with the policy of this principle, but must meet it in an alternative way. Indeed, that alternative way—direct notice to consumers, prior to the NebuAd service taking effect, with an opportunity to opt out then and persistently thereafter—may be more transparent than the Commission's proposed transparency principle.

Principle 2: To address the concern that data collected for behavioral advertising may find its way into the hands of criminals or other wrongdoers, and concerns about the length of time companies are retaining consumer data, the FTC staff proposes:

- Any company that collects or stores consumer data for behavioral advertising should provide reasonable security for that data and should retain data only as long as is necessary to fulfill a legitimate business or law enforcement need.

NebuAd Response: NebuAd is in complete agreement with this principle. While NebuAd does not collect personally-identifiable information and does not store raw data associated with individual users, NebuAd nevertheless provides state-of-the-art security for the data it does collect and store: commercial categories mapped against anonymous identifiers and some aggregate data used for analytics. Moreover, unlike some search some companies, NebuAd retains the data used for behavioral advertising purposes only for as long as it is useful for that purpose—generally from a few days to a couple of months.

Principle 3: To address the concern that companies may not keep their privacy promises when they change their privacy policies, FTC staff proposes:

- Companies should obtain affirmative express consent from affected consumers before using data in a manner materially different from promises the company made when it collected the data.

NebuAd Response: NebuAd requires by contract that its ISP partners not only change their privacy policies to address NebuAd's service, but also to provide direct notice to subscribers at least 30 days prior to the service taking effect, with an opportunity to opt-out. This allows for subscribers to exercise informed choice prior to the service taking effect. It is important to note that opting out does not mean that the subscriber must find a new ISP; rather, the subscriber may stay with the same ISP, without the NebuAd behavioral advertising service offering more relevant ads than those the subscriber would otherwise receive.

Principle 4: To address the concern that sensitive data—medical information or children's activities online, for example—may be used in behavioral advertising, FTC staff proposes:

- Companies should only collect sensitive data for behavioral advertising if they obtain affirmative express consent from the consumer to receive such advertising.

NebuAd Response: The NebuAd system does not make use of any market segments that are deemed to be sensitive. Specifically, NebuAd does not track or serve ads based on visits related to adult content, sensitive medical information, racial or ethnic origins, religious beliefs or content of a sexual nature, and does not have market segment categories for illegal products. Accordingly, the NebuAd system does not have nor does the system ever attempt to detect keyword patterns related to such subjects. NebuAd therefore looks forward to the final set of the FTC Staff's "sensitive" categories, which NebuAd assumes will be carefully tailored to prevent consumer harm, and, assuming so, will exclude those categories from the data used for behavioral advertising purposes or require an affirmative opt-in for them.

Question 2. Does your system accommodate for a consumer's choice not to receive behavioral advertising, and in your systems, is that request honored permanently? If so, please explain how.

Answer. Yes. NebuAd's service and policies were designed to provide consumers with prior, robust notice and the opportunity to express informed choice about

whether to participate, both before the service takes effect and persistently thereafter.

If a consumer should exercise his/her choice to not receive behavioral advertising, the consumer's choice is honored in the same manner as all other typical ad networks that provide "cookie-based opt-out mechanisms" and consistent with the self-regulatory guidelines of the Network Advertising Initiative ("NAI").

In addition, as stated on the opt-out page displayed to the consumer (either on the NebuAd website or on our partner ISP website), we inform that consumer that if he/she should delete the NebuAd cookie or if he/she should change computers or web browsers, then the consumer would need to opt-out again. This is similar to the statement that the members of the NAI make to consumers (*http://lwww.networkadvertising.org/managing/opt out.asp*).

NebuAd's current opt-out system is a more robust mechanism than traditional "cookie-based opt-out" systems and goes beyond the system offered by typical ad networks in the following situation. If a consumer's web browser blocks cookies, the NebuAd system will consider the consumer to be an opted-out user and will exclude that consumer from NebuAd's information collection and targeted ads.

Finally, NebuAd recently announced that it is developing a network-based opt-out mechanism that is not reliant on web browser cookies. Leveraging this advanced technology, ISP partners will be empowered to offer this enhanced mechanism to their subscribers in order to honor their opt-out choices more persistently than current systems widely used today.

Question 3. Can you expand on how NebuAd's model collects information for marketing, depersonalizes that information into market segments, and keeps it depersonalized? To be clear, I am not asking that you reveal any of your company's proprietary information, only a general overview of how this is done and how consumers' information is protected in your system.

Answer. The NebuAd system only uses a select set of a consumer's Internet activities (that is, only a subset of HTTP traffic) to construct anonymous inferences about the consumer's level of qualification for a predefined set of market segment categories ("anonymous user profiles"), which are then used to select and serve the most relevant advertisements to that consumer.

Depersonalization into Market Segments

An anonymous user profile is a set of numbers that represent the consumer's level of qualification for a predefined set of NebuAd supported market segments (*e.g.,* Las Vegas travel or domestic SUVs). NebuAd develops a set of keyword patterns associated with each specific market segment.

As HTTP traffic flows through, the NebuAd system looks for appearances of these keyword patterns. A consumer's level of qualification for each particular market segment increases for each detected keyword pattern appearance. None of a consumer's HTTP traffic or the keyword patterns themselves is ever stored within an anonymous user profile. Only the set of numbers that represent the consumer's level of qualification, at a given point in time, for a limited number of broad market segments is maintained within an anonymous user profile. This mechanism of constructing anonymous inferences about a consumer's level of qualification and not storing the raw data that was used to create or update a user's anonymous profile provides a strong additional layer of privacy protection that goes beyond the standards used by many Internet companies today.

In addition, each market segment has a predefined lifespan associated with it so if no keyword pattern for that market segment is detected for some time, the consumer's level of qualification will age fairly quickly—generally from a few days to a couple of months.

Specifically, this means that a consumer's anonymous user profile represents just his/her current qualification levels and does not retain a long-standing history of qualifications levels.

Additional Protections

The NebuAd system has also built-in multiple additional privacy protections from the ground up to ensure a consumer's anonymity including:

- The NebuAd system does not collect or use any information from password-protected sites (*e.g.,* HTTPS traffic), web mail, e-mail, instant messages, or VoIP traffic.
- As noted above, the NebuAd system does not make use of any market segments that are deemed to be sensitive. Specifically, NebuAd does not track or serve ads based on visits related to adult content, sensitive medical information, racial or ethnic origins, religious beliefs or content of a sexual nature, and does

not have market segment categories for illegal products. Accordingly, the NebuAd system does not have nor does the system ever attempt to detect keyword patterns related to such subjects.

- Finally, by design, the NebuAd system's set of keyword patterns do not contain any personally identifiable information about Internet consumers, and it ensures the anonymous information that its systems infer cannot be used to identify any individual. None of the anonymous information NebuAd uses can be compiled together and somehow reverse engineered to identify any individual. In other words, the information is not "pseudo-anonymous."

MEMORANDUM

July 8, 2008

From: Nebuad, Inc.
Re: Legal and Policy Issues Supporting Nebuad's Services

I. Introduction to NebuAd

NebuAd is an online media company founded by Internet security experts in 2006. It provides online advertising in partnership with ISPs, using a select set of a user's Internet activities (only a subset of HTTP traffic) to construct anonymous inferences about the user's level of qualification with respect to a predefined set of market segment categories ("anonymous user profiles"), which are then used to select and serve the most relevant advertisements to that user.

NebuAd is a newcomer to the world of online advertising. This world of Internet companies includes several industry giants, behavioral advertising networks, and countless website publishers. Currently, online advertising solutions operate in many locations throughout the Internet ecosystem—from users' computers to individual websites to networks of websites. When an Internet user visits the sites of web publishers, like Yahoo! or Amazon, these sites typically collect information about the user's activities to target ads based on that information. When an Internet user conducts a search, the search company may collect information from the user's activity, which in turn may be used to improve the relevance of the sponsored search results and ads shown. When a user visits websites within an online advertising network, some of which include thousands of sites, the visits help the advertising network track the user for the purpose of serving higher-value targeted advertising. All of these activities are well-entrenched in the Internet and have become fundamental to the economic model that underpins the wide availability of content and services on the Internet today. These advertising capabilities, have proven to have mutual benefits for users, publishers—both large and small—and advertisers.

NebuAd offers a unique business model that allows ISPs to participate in the online advertising ecosystem, while not only adhering to industry-standard privacy policies but also establishing new state-of-the-art privacy protections and user choice policies that go far and beyond those used on the Internet today.

Given the background of its founders, NebuAd architected its service and its policies to adhere to very strict privacy principles. These include:

1. *NebuAd's service does not collect or use PII from ISP subscribers.* The entire ad optimization and serving system does not collect or use any Personally Identifiable Information (PII), nor does it collect any information from password-protected sites, web mail, e-mail, instant messages, or VOIP traffic.

2. *NebuAd stores only a set of numbers that represent the user's level of qualification for a predefined set of market segment categories ("anonymous user profiles").* NebuAd does not store raw data such as URLs navigated or IP addresses associated with an identifiable individual.

Rather, the NebuAd service constructs anonymous inferences about the user's level of qualification for a predefined set of market segment categories, and then discards the raw data that was used to create or update a user's anonymous profile. This mechanism of constructing anonymous inferences about the user's level of qualification and not storing raw data provides a strong additional layer of privacy protection that goes beyond the standards used by many Internet companies today.

3. *NebuAd's ISP Partners are required to provide notice to users in advance of launch of the service.* The notice, which must be direct and robust, discloses to the user that the ISP is working to ensure that advertisements shown will be more relevant advertisements, that to deliver these ads its partner creates anonymous profiles based on part of the user's web surfing behavior, which does not include the collection of PII, and that the user may opt-out of the service.

For existing subscribers, the notice is required to be delivered 30 days prior to the launch of the service by postal mail, e-mail, or both. For new subscribers, the notice is required to be placed clearly and conspicuously in the new subscriber sign-up flow and outside the privacy policy. All subscribers can opt-out at any time, and on-going disclosure and opportunity to opt-out is required to be provided within the ISP's privacy policy.

4. *NebuAd and its ISP partners offer users advance and on-going choice of opting-out of the service.* Users are provided with a clear statement of what the opt-out means and the way it operates. Once the opt-out option is chosen, NebuAd honors that choice and ignores the user's subsequent web surfing activity and thus does not serve the user with behaviorally targeted ads.[1]

5. *NebuAd's service only creates anonymous user profiles, which contain no PII and no raw data, and its placement of ads is completely anonymous.* NebuAd uses proprietary algorithms and techniques, including one-way encryption of data, so that no one—not even NebuAd's engineers who designed the system—can reverse-engineer an anonymous identifier, or the anonymous user profile associated with it, to an identifiable individual.

6. *NebuAd avoids any sensitive websites or product categories.* NebuAd does not track or serve ads based on visits related to adult content, sensitive medical information, racial or ethnic origins, religious beliefs or content of a sexual nature, and does not have market segment categories for illegal products.

7. *NebuAd does not permit either complexity of data or narrowness of data to be reverse-engineered into PII.* This protection is accomplished because anonymous user profiles are constructed by anonymous inferences about the user's level of qualification for a predefined set of market segment categories. Raw data is simply not stored as part of the anonymous user profile. In addition, the NebuAd service does not have narrowly-defined segments. Finally, the anonymous profile identifier is the result of multiple encryptions, and based on multiple data elements including the hashed IP address.

8. *There is no connection or link between the ISP's registration data systems and NebuAd.* That means that no user-specific data is exchanged between NebuAd and ISP data systems. This boundary is preserved further, and inadvertent disclosure is prevented, because NebuAd immediately performs a one-way encryption of the IP address and other anonymous user identifiers used within the NebuAd system.

9. *NebuAd installs no applications of any type on users' computers, has no access to users' hard drives, and has no access to secure transactions.* As such, NebuAd does not control a user's computer or web-surfing activity in any way, *e.g.,* by changing computer settings or observing private or sensitive information.

10. *NebuAd's Data Centers are professionally operated and secured.* NebuAd's servers are located at secure sites with state-of-the-art protections against any intrusion, electronic or physical.

II. The Federal Wiretap Act

As a threshold matter, it is important to note that the Federal Wiretap Act[2] was last amended in 1986 before the widespread adoption of personal computing and online communications.[3] When the Wiretap Act was enacted, and amended, the focus was on telephone communication and other similar technology. Case law is rich with examples of claims involving a tapped phone line.[4] Notably, these cases primarily involve direct, one-on-one communication between the parties. The content is personal to the speakers, such that if one of the parties was replaced, the communication would not contain the same content. Although secrecy or confidentiality was not expressly built into the Wiretap Act, the Act was enacted at a time when the focus was on individual communications—likely as a result of the limitations of then-existing technology.

---

[1] The user, of course, will continue to receive ads.

[2] 18 U.S.C. § 2510 *et seq*.

[3] The Wiretap Act was amended by the Electronic Communications Privacy Act of 1986 ("ECPA"), Pub. L. 99–508, 100 Stat. 1848 (1986). While the Wiretap Act is Title I of the ECPA, it was first passed as Title III of the Omnibus Crime Control and Safe Streets Act of 1968 and is generally known as "Title III."

[4] *See, e.g., United States* v. *Foster,* 580 F.2d 388 (10th Cir. 1978) (telephone company taps phone line of user suspected of defrauding the telephone company out of long-distance charges); *United States* v. *Harvey,* 540 F.2d 1345 (8th Cir. 1976) (same); *United States* v. *Auler,* 539 F.2d 642 (7th Cir. 1976) (same).

The environment that has since evolved for online communications is markedly different. While online communications are still carried by wire, there are important policy distinctions between the types of communications that the Wiretap Act was enacted to address, and the types of communications present in the online environment today. Internet users are not engaged in a personal, direct conversation with non-secure website publishers.[5] Such publishers provide online content indiscriminately to all users. As stated below, even under the Wiretap Act, courts look to the circumstances surrounding a communication.[6] Yet, the evaluation of circumstances that surround a telephone communication between two parties is not analogous to an online communication between a party and a website. To date, there are no litigated decisions directly addressing the application of the Wiretap Act to a URL provided as part of a consumer's online navigations or provided via publicly available search request and response. Therefore, it is still an open question as to whether these types of communications are even covered by the Wiretap Act.[7]

Assuming, for the purposes of this memorandum, that the Wiretap Act applies to NebuAd's services, the Act expressly prohibits the intentional interception of an electronic communication[8] unless "one of the parties to the communication has given prior consent to such interception."[9] The legislative history of the Wiretap Act clearly indicates "that Congress intended the consent requirement to be construed broadly."[10] As a result, "courts have resoundingly recognized the doctrine of implied consent."[11] The Court of Appeals for the Second Circuit stated that the Wiretap Act "affords safe harbor not only for persons who intercept calls with the explicit consent of a conversant but also for those who do so after receiving implied consent."[12]

To determine whether a party has impliedly consented to an interception under the Wiretap Act, courts examine the totality of the circumstances and "imply consent in fact from surrounding circumstances indicating that the [party] knowingly agreed to the surveillance."[13] In such evaluations, courts have found that parties impliedly consented to an interception in various fact patterns. The Federal district court for the Southern District of New York found implied consent when an employer circulated memoranda regarding telephone monitoring and recording. Although the party denied receiving the notice, and evidence proving such receipt was destroyed, the court determined that the party had knowledge of the monitoring and recording and impliedly consented to such monitoring and recording by continuing to use the monitored telephone lines.[14]

Similarly, a Connecticut Federal district court found that employees had given their implied consented to the recording of conversations on work telephones, as many of the telephones displayed warning labels, memoranda were circulated to all employees regarding the recordingof incoming and outgoing telephone calls.[15] The court stated that employees' "knowledge of the system and subsequent use of the phones is tantamount to implied consent to the interception of their conversa-

---

[5] There are always exceptions to this statement, such as online purchases, encrypted communication, and other secured data transactions, but notably, these private communications are the exact types of information that NebuAd's services do not collect. NebuAd's services personalize generic content rather than intruding upon private communications.

[6] *See United States* v. *Amen,* 831 F.2d 373, 378 (2d Cir. 1987).

[7] *See* Patricia L. Bellia, *Spyware: The Latest Cyber-Regulatory Challenge,* 20 BERKELEY TECH. L.J. 1283, 1296, 1311–12 (2005). Another law review article described the question as to whether URLs contain contents as "surprisingly difficult" and "quite murky." Orin S. Kerr, *Internet Surveillance Law After the USA Patriot Act: The Big Brother That Isn't,* 97 NW. U.L. REV. 607, 645–46 (2003).

[8] 18 U.S.C. § 2511(1)(a).

[9] *Id.* § 2511(2)(d).

[10] *United States* v. *Amen,* 831 F.2d 373, 378 (2d Cir. 1987) ("'Consent may be expressed or implied. Surveillance devices in banks or apartment houses for institutional or personal protection would be impliedly consented to.'" (quoting S. Rep. No. 1097, 90th Cong. 2d Sess., *reprinted in* 1968 U.S.C.C.A.N. 2112, 2182)).

[11] *George* v. *Carusone,* 849 F. Supp. 159, 164 (D. Conn. 1994); *see United States* v. *Faulkner,* 439 F.3d 1221, 1224–25 (10th Cir. 2006) ("We are not persuaded to depart from the unanimous view of the *holdings* by our fellow circuit courts."); *Griggs-Ryan* v. *Smith,* 904 F.2d 112, 118; *United States* v. *Corona-Chavez,* 328 F.3d 974, 978–79 (8th Cir. 2003); *Amen,* 831 F.2d at 378; *United States* v. *Willoughby,* 860 F.2d 15, 19–20; *United States* v. *Tzakis,* 736 F.2d 867, 870, 872 (2d Cir. 1984); *Borninski* v. *Williamson,* No. Civ. A. 3:02CV1014–L, 2005 WL 1206872, at *13 (N.D. Tex. May 17, 2005); *United States* v. *Rittweger,* 258 F. Supp. 2d 345, 354 (S.D.N.Y. 2003); *Chance* v. *Avenue A, Inc.,* 165 F. Supp. 2d 1153, 1162 (W.D. Wash. 2001); *In re DoubleClick Inc. Privacy Litig.*, 154 F. Supp. 2d 497, 514 (S.D.N.Y. 2001).

[12] *Griggs-Ryan,* 904 F.2d at 116.

[13] *Amen*, 831 F.2d at 378.

[14] *Rittweger,* 258 F. Supp. 2d at 354.

[15] *George,* 849 F. Supp. at 164.

tions."[16] The Court of Appeals for the First Circuit held that repeated oral statements that all incoming telephone calls would be monitored was sufficient notice, and that the party's taking an incoming phone call was implied consent to the interception.[17] Additionally, a Texas Federal district court found that an employee consented to monitoring of Internet communications at work because the employee had signed a form stating that "Internet access should be limited to 'business use only,' and that the company 'logs and archives all incoming and outgoing data communications through its gateway system. Use of the gateway implies consent to such monitoring.'"[18]

Using the framework established by the courts, NebuAd satisfies the implied consent exception to liability for interception under the Federal Wiretap Act.[19] NebuAd requires, by contract, that all of its ISP partners give subscribers notice of NebuAd's services, including the collection of anonymous information regarding subscribers' online activities, for use in advertising. This notice must be given directly, and prior to the initiation of the ISP's use of NebuAd's services. The ISP partners are also required, by contract, to alter their privacy policies accordingly. NebuAd further requires that all ISP partners provide users with an option to opt-out of NebuAd's services, initially upon receipt of the direct notice, and in an ongoing manner through the ISP's privacy policy.

III. The Cable Act

The Cable Act[20] was enacted to protect cable subscribers' personal information. Among other things, it requires cable operators to obtain written or electronic consent from a subscriber prior to collecting any PII concerning the subscriber.[21] In addition to the limitations on the collection of subscriber PII, the Cable Act limits the disclosure of subscriber PII by cable operators.[22] The Cable Act sets out multiple standards that a cable operator must satisfy in order to disclose subscriber PII. If the disclosure is necessary for a legitimate business activity, a cable operator is not required to provide the subscriber with any notice.[23] A cable operator may disclose the name and mailing addresses of subscribers if it provides subscribers with the opportunity to opt out of such disclosure.[24] For all other disclosures of subscriber PII, a cable operator must obtain "the prior written or electronic consent of the subscriber"—essentially an opt-in standard.[25]

Notably, under the Cable Act, PII "does not include any record of aggregate data which does not identify particular persons."[26] NebuAd's service specifically complies with the Cable Act because NebuAd's service does not collect PII. Instead, using only non-personally identifiable information, NebuAd uses a select set of a user's Internet activities (a subset of HTTP traffic) to construct anonymous inferences about the user's level of qualification for a predefined set of market segment categories, which are then used to select and serve the most relevant advertisements to that user. The use of NebuAd's services certainly does not require a subscriber to opt in—the strictest notice and consent requirement. Although not an activity conducted by NebuAd, even the disclosure of a subscriber's mailing address, widely recognized as PII, only requires that the subscriber have an opportunity to opt out. NebuAd's service, on the other hand, does not even collect subscriber PII. Because NebuAd's service does not collect subscriber PII, there is no violation of the Cable Act.

Additionally, a 2002 FCC ruling concluded that "cable modem service, as it is currently offered, is properly classified as an interstate information service, not as a cable service, and that there is no separate offering of a telecommunications serv-

---

[16] *Id.*
[17] *Griggs-Ryan,* 904 F.2d at 117–19.
[18] *Borninski* v. *Williamson,* No. Civ. A. 3:02CV1014–L, 2005 WL 1206872, at *13 (N.D. Tex. May 17, 2005).
[19] Website publishers may also consent to an interception, as website publishers make web content available for any user. Such posting does not constitute an exclusive communication between the website publisher and the user, but rather it is public communication that is intended to be viewed by any number of simultaneous users. As a result, website publishers have no reasonable expectation that the communication between it and any consumer will remain private or confidential, and thus impliedly consent to the interception by a third party.
[20] Cable Communications Policy Act (1984), 47 U.S.C. § 551 *et seq.*
[21] *Id.* § 551(b)(1).
[22] *Id.* § 551(c).
[23] *Id.* § 551(c)(2)(A).
[24] *Id.* § 551(c)(2)(C)(i).
[25] *Id.* § 551(c)(1).
[26] *Id.* § 551(a)(2)(A).

ice."[27] This determination that cable Internet services are not classified as telecommunications services was upheld by the Supreme Court as a lawful interpretation of the Communications Act.[28] A recent decision by the Court of Appeals for the Sixth Circuit upheld this distinction and stated that the plain language of the Cable Act precludes its application to broadband Internet services, even those provided by a cable operator.[29] Examining the application of the Cable Act, the court emphasized that as the cable provider was providing broadband Internet access and not cable service, the Cable Act was inapplicable.

IV. Policy Implications

NebuAd provides users with a great amount of privacy protection. Unlike many online advertising models today, NebuAd's service does not collect or use any PII. In addition, NebuAd's anonymous user profiles do not contain any original raw data, such as URLs navigated, but only consist of a set of numbers that represent anonymous inferences about the user's level of qualification for a predefined set of market segment categories. (NebuAd does retain some anonymous data for analysis and reporting.) Additionally, NebuAd is one of the only models—if not the only model—that provides users with advance notice of the nature of its services and an opportunity to opt-out *before* the service takes effect. NebuAd's service also complies with the government's consent policy on privacy as NebuAd's service does not collect any PII, and provides users with the opportunity to opt-out.[30] Finally, NebuAd's service does not observe encrypted traffic, does not observe VoIP sessions, does not store raw search queries linked to an identifiable user, and does not track users' IP addresses, thus providing an excellent set of privacy protections. Because of the privacy protections that NebuAd has incorporated into the architecture of its service, it is able to provide users with relevant advertising messages in a safe, secure, and privacy-respecting manner.

MEMORANDUM ADDENDUM

July 8, 2008

From: Nebuad, Inc.
Re: Legal and Policy Issues Supporting Nebuad's Services

I. The Memorandum on Behavioral Advertising[1] by the Center For Democracy and Technology Is Based on a Misunderstanding of Nebuad's Services

NebuAd's service was architected to comply with very strict privacy principles. The Center for Democracy and Technology ("CDT") misunderstands how NebuAd's service operates. First, the service does not "cop[y] all or substantially all Web transactions."[2] NebuAd's service uses only a subset of HTTP traffic to construct anonymous inferences about the user's level of qualification with respect to a predefined set of market segment categories. NebuAd's service only stores a one-way encrypted anonymous user identifier, which is used to represent an anonymous user, and a set of numbers which represent the user's level of qualification with respect to a predefined set of market segment categories. NebuAd does not store raw data such as URLs navigated or IP addresses associated with an identifiable individual. Second, to provide additional privacy protection, NebuAd's service does not track or serve ads based on visits to sensitive websites or product categories. CDT also unfortunately erroneously stated in its Memorandum that a NebuAd ISP implementation "did not provide a way for subscribers to give or withhold consent."[3] This is not so. NebuAd requires its ISP partners, by contract, to give their ISP sub-

---

[27] *In re Inquiry Concerning High-Speed Access to the Internet Over Cable and Other Facilities,* 17 FCCR 4798, 4802 (2002).

[28] *Nat'l Cable and Telecomms. Ass'n* v. *Brand X Internet Servs.,* 545 U.S. 967 (2005).

[29] *Klimas* v. *Comcast Cable Commc'ns, Inc.,* 465 F.3d 271 (6th Cir. 2007), *reh'g en banc denied Klimas* v. *Comcast Cable Commc'ns, Inc.,* 2007 U.S. App. LEXIS 13658 (6th Cir. May 1, 2007).

[30] Use of a consumer opt out is consistent with other consumer information protection statutes such as the Gramm-Leach-Bliley Act (financial data), the Health Insurance Portability And Accountability Act (health data), the Fair Credit Reporting Act (consumer reports), the Telemarketing and Consumer Fraud and Abuse Prevention Act (telemarketing), and the CAN–SPAM Act (e-mail marketing).

[1] Center for Democracy and Technology, Privacy Implications of Online Advertising (July 9, 2008) [hereinafter "CDT Memorandum"].

[2] CDT Memorandum at 23.

[3] *Id.* at 15.

scribers prior, direct notice about NebuAd's service and an opportunity to withhold consent or to express their informed choice before the service takes effect.

II. The CDT's Evaluation Is Largely a Policy Argument on How the Existing Law Ought to Apply in the Internet Context

A. Federal Wiretap Act

While citing a number of cases and policy arguments, the CDT acknowledges that exceptions to the Federal Wiretap Act may apply. The CDT Memorandum contains hedging language that an exception "probably does not permit" NebuAd's service,[4] that it is "unlikely" that the "necessary incident" exception would apply,[5] and citing no cases on point, that it is "unclear" whether the "business use" exception would apply.[6] It is therefore unclear from the CDT's own Memorandum whether NebuAd's service qualifies for either of these exceptions.

The CDT also does not deny that implied consent, where a consumer receives notice, prior to the service taking effect, has the opportunity to opt-out, and continues to use the service, can and often amounts to implied consent under the Wiretap Act, which has been well-recognized by the Federal courts. The CDT Memorandum equivocates on NebuAd's service in particular, stating that prior notice of NebuAd's service "might not be enough," [7] to meet the implied consent standard, and that the courts would be skeptical "if" the notice to consumers did not provide sufficient notice of the services.[8]

The CDT's Memorandum does not give a full picture of the implied consent standard. While courts have stated "that consent under the Wiretap Act 'is not to be cavalierly implied,'" [9] courts have equally stated that "Congress intended the consent requirement to be construed broadly." [10] These statements are not mutually exclusive, and courts have made both statements in the same case.[11]

Moreover, none of the cases the CDT relies on for its policy argument that opt-in should be required is on point, and some contain language affirming the use of implied consent. For example, reliance on *Watkins* [12] for the proposition that implied consent is insufficient is misplaced, as *Watkins* involves an employee that had consented to limited monitoring practices by an employer, and the employer subsequently exceeded the authorized monitoring. Thus, *Watkins* does not state that implied consent is invalid, but rather that consent may be limited.[13] Similarly, the CDT cites to *Griggs-Ryan* v. *Smith* [14] for the proposition that "consent should not casually be inferred." The context surrounding this statement is important in order to gauge the statement's full meaning. In the preceding paragraphs of the same case, the court described how "Congress intended the consent requirement to be construed broadly," and "that Title III affords safe harbor not only for persons who intercept calls with the explicit consent of a conversant but also for those who do so after receiving implied consent." [15] The *Griggs-Ryan* court found implied consent based on repeated oral statements that all incoming calls would be monitored. The other cases CDT cites on implied consent are either distinguishable or don't apply here.[16]

---

[4] *Id.* at 26.
[5] *Id.* at 26.
[6] *Id.* at 27.
[7] *Id.* at 30–31.
[8] *Id.* at 31.
[9] *Id.* At 30 (quoting *Watkins* v. *L.M. Berry & Co.,* 704 F.2d 577, 579 (11th Cir. 1983).
[10] *Griggs-Ryan* v. *Smith,* 904 F.2d 112, 116 (1st Cir. 1990); *see, e.g., United States* v. *Amen,* 831 F.2d 373, 378 (2d Cir. 1987); *United States* v. *Faulkner,* 439 F.3d 1221, 1224 (10th Cir. 2006); *George* v. *Carusone,* 849 F. Supp. 159, 164 (D. Conn. 1994).
[11] *See, e.g., Griggs-Ryan* v. *Smith,* 904 F.2d at 116–17.
[12] *Watkins* v. *L.M. Berry & Co.,* 704 F.2d 577 (11th Cir. 1983).
[13] *See also Griggs-Ryan,* 904 F.2d at 119 (finding the plaintiff's heavy reliance on *Watkins* to be mislaid because of the limited consent in that case).
[14] *Griggs-Ryan,* 904 F.2d 112 (1st Cir. 1990).
[15] *Id.* at 116.
[16] *See Pharmatrak, Inc. Privacy Litig.,* 329 F.3d 9, 19–20 (1st Cir. 2003) (The court found that "consent must be actual, not constructive." The court in *Pharmatrak* indeed made this point but only insofar as to cite to the decision from which it originated, namely, *Williams* v. *Poulos,* 11 F.3d 271 (1st Cir. 1993).); *United States* v. *Corona-Chavez,* 328 F.3d 974, 978 (8th Cir. 2003) (The court held that there must be actual consent to meet the consent exception under the Wiretap Act. The court provides the example that "when someone voluntarily participates in a telephone conversation knowing that the call is being intercepted, this conduct supports a finding of implied consent to the interception."); *Berry* v. *Funk,* 146 F.3d 1003, 1011 (D.C. Cir. 1998) (The court found that "[w]ithout actual notice, consent can only be implied when the surrounding circumstances convincingly show that the party knew about and consented to the interception." In this case, the government tried to show implied consent by arguing that any

B. State Wiretap Statutes

In addition to noting various all-party consent states, the CDT has focused on California. First, the CDT Memorandum contains hedging language regarding the application of various exceptions, such that if such an exception were met, the issue of all-party consent would not be reached as NebuAd's service would be exempted from liability under alternative grounds.[17] Additionally, the CDT notes the lack of developed case law on the extension of the California wiretap statute to Internet communications.[18] The CDT points to the extraterritorial application of the California wiretap statute involving telephone communications—notably after recognizing that such statute may be inapplicable to NebuAd's service—but then offers a countervailing argument that California's consent requirement may be inapplicable to behavioral advertising altogether.[19] While focusing on the California wiretap statute as a roadblock to NebuAd's service, the CDT Memorandum itself recognizes that the statute may exempt NebuAd's service or may be inapplicable to the industry altogether.

RESPONSE TO WRITTEN QUESTION SUBMITTED BY HON. DAVID VITTER TO CLYDE WAYNE CREWS, JR.

Question. As our Committee continues to examine the issue of online privacy, should we focus on the variations in different technologies used to provide what appears to be essentially similar marketing services? Or, should we instead focus on the use of the information collected—by whatever method it is collected—to ensure that data is used for legitimate marketing purposes, that privacy is protected, and that we can go after those who misuse any data they collect?

Answer. Targeted marketing encompasses a diverse array of relationships between users, marketers, and websites. While all types of behavioral advertising techniques are often lumped together, there is in fact a great deal of variety among online marketing business models.

Even across search engines, there is no uniform method of dealing with user data from search queries. Google, for example, to improve search accuracy by recording every search query along with the user's IP address and the time the search was conducted. Yet, Google does not utilize this data to create user profiles. Another search provider, the recently launched Cuil, does not retain any personal data. Microsoft recently unveiled plans to deliver search results that take into consideration each user's individual browsing habits, arguing that Microsoft's Live Search engine will be better equipped to compete against Google if it can analyze the intent of each user.

The misuse of sensitive information is an important concern for policymakers evaluating online privacy issues. However, misuse can only be defined on a case-by-case basis. This cannot be accomplished by prescriptive legislation—especially in frontier sectors like the Internet. The danger of stifling nascent markets is far greater than any potential benefits of legislation which privacy mandates could bring.

Controversial practices like the use of deep-packet inspection by Internet Service Providers may offer commercial opportunities with benefits to consumers. Lower broadband bills are just one possible benefit from the delivery of personalized ads to subscribers. Of course, for many users, privacy concerns trump potential benefits. In some instances, firms may inaccurately assess consumer preferences, resulting in mistakes like the NebuAd scuffle. Such mistakes, however disturbing, will be resolved by market forces as competing firms respond to consumer concerns by revising data collection practices as needed.

Consider two users with different levels of concern regarding personal privacy. One user lists his hobbies, friends, and demographic details on a public social net-

---

reasonable person would assume that an operator stayed on the line if not told otherwise. In dismissing this argument, the court found that "[t]he key question in such an inquiry obviously is whether parties are given sufficient notice."); *Deal* v. *Spears,* 980 F.2d 1153 (8th Cir. 1992) (holding that a warning about the possibility, rather than actual notice, of monitoring did not constitute sufficient notice for implied consent); *Specht* v. *Netscape Commc'ns Corp.,* 306 F.3d 17 (2d Cir. 2002) (evaluating claims outside the Wiretap Act and considering the sufficiency of notice provided by an inconspicuous software download license agreement); *United States* v. *Lanoue,* 71 F.3d 966, 981 (1st Cir. 1995) (standing for the general proposition that "[d]eficient notice will almost always defeat a claim of implied consent," this acknowledges that sufficient notice will support a finding of implied consent).

[17] *See supra* notes 4–8 and accompanying text.

[18] CDT Memorandum at 33.

[19] *Id.*

working profile and does not expect that data to remain private. On the other hand, another user whose Gmail inbox contains sensitive personal correspondence assumes the data will not be made public. In the current environment—where government enforces voluntary privacy arrangements, but does not dictate them—both users can be satisfied. Thanks to Gmail's robust privacy policy, the concerned user can rest assured that her e-mails will be safe from outside prying. And the user of the social networking site can enjoy the services and content sustained by marketing income without undesired rules preventing the use of data that is clearly in the public sphere.

The technologies that drive online advertising are incredibly complex, and new ways of analyzing data are constantly being developed. Therefore, the fundamental question in the online privacy debate is *how we arrange* for our data to be used once it has been transferred to a third party. Calls for Congress to build walls around personal information would preclude these arrangements, giving us too little privacy in some cases and too much in others. A set of guidelines that seems reasonable when applied to ISP deep-packet inspection might eliminate other, more innocuous business models that rely on targeted marketing.

RESPONSE TO WRITTEN QUESTIONS SUBMITTED BY HON. DAVID VITTER TO MICHAEL D. HINTZE

Thank you again for your interest in the important privacy implications of online advertising. Microsoft has a deep and longstanding commitment to consumer privacy issues, and we welcomed the opportunity to testify before the Senate Commerce Committee about the concrete steps we are taking to protect consumers' privacy online. As we indicated in our testimony, Microsoft believes that strong privacy protections are not only compatible with bringing the benefits of online advertising to consumers, advertisers and publishers, but are essential to ensuring the success of this important business model. This means that Microsoft, and all companies operating online, must adopt meaningful privacy practices that build trust with consumers. We believe our responses to your important follow-up questions demonstrate that Microsoft takes this responsibility seriously.

Question 1. Does your company's business model already accommodate the FTC's proposed principles for industry self-regulation? If so, please explain how.

Answer. Yes, Microsoft's business model accommodates and even exceeds the Federal Trade Commission's proposed principles for self regulation. In our comments to the FTC, we urged the Commission to focus on a broad array of online advertising activities (not simply behavioral advertising) because all online advertising involves the collection of data about computer users and may be contrary to consumers' expectations.[1] To this end, Microsoft specifically advocated for a tiered approach to self regulation that is appropriately tailored to account for the types of information being collected and how that information will be used. Our proposal would establish a baseline set of privacy protections applicable to all online advertising activities and additional obligations for those companies that engage in practices that raise additional privacy concerns.

Microsoft's broad approach to self regulation is based on the comprehensive privacy principles for online search and ad targeting we announced in July 2007.[2] These principles include commitments to user notice, user controls, anonymization, security, and best practices. Microsoft has embraced these privacy principles, and they will shape the development of our new product offerings. We also have released a set of privacy guidelines designed to help developers build meaningful privacy protections into their software programs and online services.[3] The following paragraphs highlight the ways in which we have implemented our own privacy principles into practice and, by doing so, have also accommodated the FTC's proposed principles for industry self-regulation.

A. *Transparency*. Microsoft agrees with the FTC that transparency is critical to enable consumers to make informed choices. To this end, Microsoft's Online Privacy Statement is readily accessible from every page of our websites, including the home page. It also is written in clear language and offered in a "layered" format that provides consumers with the most important information about our privacy practices upfront, followed by additional layers of notice that provide a more comprehensive

---

[1] *See http://www.ftc.gov/os/comments/behavioraladprinciples/080411microsoft.pdf.*

[2] Microsoft's Privacy Principles for Live Search and Online Ad Targeting are available at *http://www.microsoft.com/mscorp/twc/privacy/default.mspx.*

[3] Microsoft's Privacy Guidelines for Developing Software Products and Services are available at *http://www.microsoft.com/privacy.*

examination of our general privacy practices.[4] With respect to the delivery of advertisements online, the Microsoft Online Privacy Notice Highlights clearly informs users about Microsoft's online advertising practices, noting that Microsoft "use[s] cookies and other technologies to keep track of your interactions with our sites and services to offer a personalized experience" and that Microsoft's services "may include the display of personalized content and advertising." In addition, our full privacy statement includes complete descriptions of the types of information collected for online advertising and the ways in which such information may be used. We believe our upfront and more detailed privacy statements help ensure consumers are fully informed of our data collection and usage practices.

B. *Consumer Control.* Microsoft also agrees with the FTC that the collection of information about consumers to generate a profile of their behavior upon which ads can be targeted raises heightened concerns that warrant additional levels of user control. For this reason, Microsoft has taken the following steps:

- Microsoft was the first major online advertising provider to announce it would give customers the opportunity to opt out of receiving targeted advertising on all of the websites where Microsoft provided advertising, including both Microsoft sites and third-party partner websites.
- Microsoft prominently provides information and links to our opt-out mechanism in the top-layer of our privacy statement and in our full privacy statement.
- Microsoft allows users to tie their opt-out choice to their Windows Live ID so their choice will be effective across multiple computers without any additional effort on the user's part.
- Microsoft's opt-out method is more persistent than others—for example, deleting cookies will not erase consumer's opt-out selection; rather, their opt-out choice will be reset when they sign in with their Windows Live ID.

We also recently announced three features of our new Internet Explorer product that will improve consumer control. First, users may choose to activate InPrivate browsing so their web surfing history, temporary Internet files, and cookies are not recorded on their computer after browsing. Second, users are given notice and a choice about whether they want to block content coming from third parties that may track and aggregate their online behavior by using the InPrivate Blocking feature. Third, users have the choice to clear all or some of their browsing history by using the enhanced Delete Browsing History feature.

C. *Security*. Microsoft is committed to the FTC's principles around data security. We have adopted strong data security practices, implemented meaningful data protection and security plans, and undertaken detailed third-party audits. We also have taken steps to educate consumers about ways to protect themselves while online, and we have worked closely with industry members and law enforcement around the world to identify security threats, share best practices, and improve our coordinated response to security issues.

D. *Data Retention*. Microsoft supports the FTC's principle that entities that collect data through online advertising "should retain data only as long as is necessary to fulfill a legitimate business or law enforcement need." As the Commission notes, there are often sound and legitimate business reasons for retaining data collected from users. These reasons include enhancing fraud detection efforts, helping guard consumers against security threats, understanding website usage, improving the content of online services, and tailoring features to consumer demands.

Microsoft's policy around retaining search query data provides a good example of the careful balance of interests that must be taken into account when analyzing retention periods. Specifically, Microsoft has committed to make search query data anonymous after 18 months by permanently removing cookies, the entire IP address, and other identifiers from search logs, unless the user has provided consent for us to retain data for a longer period of time. Unlike other companies, our anonymization method involves irreversibly removing the *entire* IP address and other cross-session identifiers, such as cookies and other machine identifiers, from search terms. Some companies remove only the last few digits of a consumer's IP address, which means that an individual search query may still be narrowed down to a small number of computers on a network. We think that such partial methods do not fully protect consumer privacy, so we have chosen an approach that renders search terms truly and irreversibly anonymous.

E. *Use of Personal Information for Online Advertising.* Microsoft agrees with the FTC that the merger of personally identifiable information with other information

[4] Microsoft's Online Privacy Statement can be found at *http://go.microsoft.com/fwlink/?LinkId=74170*.

collected about consumers through behavioral advertising for the purposes of ad targeting presents further privacy risks. This is because consumers are unlikely to expect that a third party may combine such pieces of information and use it to deliver ads (whether online or offline). For this reason, Microsoft has developed its online ad targeting platform to select appropriate ads based only on data that does not personally and directly identify individual users, and we take steps to separate the data used for ad targeting from any personally identifiable information before using it to serve ads—a process we refer to as "deidentification."[5] Specifically, for users who have created Windows Live accounts, rather than using the account ID as the basis for our ad systems, we use a one-way cryptographic hash to create a new anonymized identifier. We then use that identifier, along with the non-identifiable demographic data, to serve ads online. Search query data and web surfing behavior used for ad targeting is associated with this anonymized identifier rather than an account identifier that could be used to personally and directly identify a user.

Question 2. Does your system accommodate for a consumer's choice not to receive behavioral advertising, and in your systems, is that request honored permanently? If so, please explain how.

Answer. Yes, Microsoft's system does accommodate for a consumer's choice not to receive behavioral advertising. In July 2007, Microsoft was the first major online advertising provider to announce it would give customers the opportunity to opt out of receiving targeted advertising on *all* of the websites where Microsoft provides advertising, including both Microsoft sites and third-party partner websites. This opt-out option became available in the Spring of 2008. We prominently provide information and links to our opt-out mechanism in the top-layer of our privacy statement and in our full privacy statement.

Microsoft's opt-out choice is also unique from any other offered in industry today because it is more persistent and applies across multiple computers. As background, the industry-standard approach for offering an opt-out choice is merely to place an "opt-out" cookie on their machines. While this process generally works well, it does have some inherent limitations. For example, opt-out cookies are computer-specific—if a consumer switches computers, he or she will need to specify any opt-out preferences again. Similarly, if cookies are deleted, that user's opt-out choice is no longer in effect. To address these limitations, the mechanism Microsoft offers gives consumers the option to associate their opt-out choice to their Windows Live ID. This means that even if they delete cookies on their machine, when they sign back in their opt-out choice will persist. It also means that a single choice can apply across multiple computers that they use. This will help ensure that consumers' choices are respected without requiring undue effort on their part.[6]

Microsoft appreciates the opportunity to provide more information about our privacy practices. We look forward to continuing to work with you and all stakeholders to ensure consumers' privacy is protected online.

○

[5] Microsoft's "de-identification" white paper is available at *http://www.microsoft.com/privacy*.

[6] Microsoft's opt-out page is available at *https://choice.live.com/advertisementchoice/Default.aspx*.